02 D0 #3

520.38691X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): KAMINAGA, et al.

Serial No.: 09/599,005

Filed: June 22, 2000

Title: INFORMATION PROCESSING DEVICE, CARD DEVICE AND INFORMATION PROCESSING SYSTEM

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

July 21, 2000

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 11-178750
Filed: June 24, 1999

A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/ssr
Attachment

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年　６月２４日

出願番号
Application Number: 平成１１年特許願第１７８７５０号

出願人
Applicant (s): 株式会社日立製作所
株式会社日立超エル・エス・アイ・システムズ

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　６月１６日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４５６５０

【書類名】　特許願

【整理番号】　PNT990072

【提出日】　平成11年 6月24日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 12/14320

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

【氏名】　神永　正博

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

【氏名】　遠藤　隆

【発明者】

【住所又は居所】　東京都国分寺市東恋ケ窪一丁目２８０番地　株式会社日立製作所中央研究所内

【氏名】　大木　優

【発明者】

【住所又は居所】　東京都小平市上水本町５丁目２２番１号　株式会社日立超エル・エス・アイ・システムズ内

【氏名】　塚元　卓

【発明者】

【住所又は居所】　東京都小平市上水本町５丁目２２番１号　株式会社日立超エル・エス・アイ・システムズ内

【氏名】　渡瀬　弘

【発明者】

【住所又は居所】　東京都小平市上水本町五丁目２０番１号　株式会社日立製作所半導体グループ内

【氏名】　寺内　千晶

【発明者】
【住所又は居所】　東京都小平市上水本町五丁目２０番１号　株式会社日立製作所半導体グループ内
【氏名】　中田　邦彦
【発明者】
【住所又は居所】　東京都小平市上水本町五丁目２２番１号　株式会社日立超エル・エス・アイ・システムズ内
【氏名】　長崎　信孝
【発明者】
【住所又は居所】　東京都小平市上水本町５丁目２２番１号　株式会社日立超エル・エス・アイ・システムズ内
【氏名】　平　聡
【発明者】
【住所又は居所】　東京都小平市上水本町５丁目２２番１号　株式会社日立超エル・エス・アイ・システムズ内
【氏名】　成吉　雄一郎
【発明者】
【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
【氏名】　福澤　寧子
【特許出願人】
【識別番号】　000005108
【氏名又は名称】　株式会社日立製作所
【特許出願人】
【識別番号】　000233169
【氏名又は名称】　株式会社日立超エル・エス・アイ・システムズ
【代理人】
【識別番号】　100061893
【弁理士】

【氏名又は名称】　高橋　明夫

【電話番号】　03-3661-0071

【選任した代理人】

【識別番号】　100086656

【弁理士】

【氏名又は名称】　田中　恭助

【電話番号】　03-3661-0071

【手数料の表示】

【予納台帳番号】　011626

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】　情報処理装置、カード部材および情報処理システム

【特許請求の範囲】

【請求項１】　情報処理装置と、当該第１の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とする情報処理装置。

【請求項２】　第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第１もしくは第２の情報処理装置の少なくとも一方よりの信号を伝達する前記信号線での第１の電力の消費状態に対応して第２の電力の消費状態が定められ、且つ前記信号線での第１の電力の消費と前記第２の電力の消費とが互いに相反する期間に可能とされていることを特徴とする情報処理装置。

【請求項３】　情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置の信号を伝達する前記信号線での第１の電力の消費状態に対応して第２の電力の消費状態が定められ、且つ前記信号線での第１の電力の消費と前記第２の電力の消費との和が所望値となされるごとく構成されたことを特徴とする情報処理装置。

【請求項４】　情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置の信号を伝達する前記信号線での第１の電力の消費状態に対応して第２の電力の消費状態が定められ、且つ前記信号線での第１の電力の消費がなされる期間では、前記第２の電力の消費がなされず、前記信号線での第１の電力の消費がなされない期間では第２の電力の消費が可能とされていることを特徴とする情報処理装置。

【請求項５】　情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置のディジタル信号を伝達する前記信号線での信号値の反転に対応して電力の消費が可能とされていることを特徴とする情報処理装置。

【請求項６】　第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第１もしくは第２の情報処理装置の少なくとも一方よりのディジタル信号に基づく前記信号線での第１の電力の消費状態に対応して、前記信号線での転送信号の信号値の反転に対応して第２の電力の消費がなされる手段を有することを特徴とする情報処理装置。

【請求項７】　情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置と前記信号線との間において、前記情報処理装置よりの信号を暗号化が可能であり且つ前記信号線より暗号化されて転送される信号を復号化することが可能なことを特徴とする情報処理装置。

【請求項８】　第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第１の情報処理装置あるいは第２の情報処理装置の少なくとも１者と前記信号線との間において、前記第１の情報処理装置あるいは第２の情報処理装置よりの信号を暗号化し、且つ前記信号線より転送されてくる信号を復号化することが可能なことを特徴とする情報処理装置。

【請求項９】　第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線とを少なくとも有し、前記第１の情報処理装置よりの信号を暗号化し、当該暗号化された第１の情報処理装置よりの信号を復号化して第２の情報処理装置に入力し、且つ前記第２の情報処理装置の出力を暗号化し、当該暗号化された第２の情報処理装置よりの信号を復号化して第１の情報処理装置に入力することが可能なことを特徴とする情報処理装置。

【請求項１０】　情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを少なくとも有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報の復号化が可能なことを特徴とする情報処理装置。

【請求項１１】　情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを少なくとも有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報を復号化して、前記信号線を介して前記情報処理装置に入力が可能なことを特徴とする情報処理装置。

【請求項１２】　情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの出力される信号列が、その順序を異にして前記信号線を伝達され、且つ前記信号列の異にされた順序を復元が可能なことを特徴とする情報処理装置。

【請求項１３】　第１のデータ処理装置と、第２のデータ処理装置と、この両者を接続する信号線と、制御信号発生手段と、前記信号線で消費される第１の電力と、当該信号線での電力消費とは別の第２の電力を消費する手段とを少くなくとも有し、前記第１あるいは第２のデータ処理装置は前記第２の電力を消費する手段に接続され、前記制御信号発生手段よりの制御信号によって当該信号線に搭載された信号をクリアしない制御方式で制御され、前記第１と第２のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第１の電力消費と前記第２の電力消費の和が所定値になるように、前記制御信号発生手段からの信号に応じて、前記第１あるいは第２のデータ処理装置から出力された信号と、当該信号の転送の直前に前記信号線に乗っている信号と、当該信号の転送の直前に充放電装置に入力された信号に対して、排他的論理和を求め、その出力信号を前記第２の電力を消費する手段への入力が可能なことを特徴とする情報処理装置。

【請求項１４】　第１のデータ処理装置と、第２のデータ処理装置と、この両者を接続する信号線と、制御信号発生手段と、前記信号線で消費される第１の電力と、当該信号線での電力消費とは別の第２の電力を消費する手段とを少くなくとも有し、前記第１および第２のデータ処理装置は各々前記第２の電力を消費する第１の手段および前記第２の電力を消費する第２の手段に接続され、前記制御信号発生手段よりの制御信号によって当該信号線に搭載された信号をクリアしない制御方式で制御され、前記第１と第２のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第１の電力消費と前記第２の電力消費の和が所定値になるように、前記制御信号発生手段からの信号に応じて、前記第１あるいは第２のデータ処理装置から出力された信号と、当該信号の転送の直前に前記信号線に乗っている信号と、当該信号の転送の直前に充放電装置に入力された信号に対して、排他的論理和を求め、その出力信号を前記第２の電力を消費する手段への入力が可能なことを特徴とする情報処理装置。

【請求項１５】　前記第２の電力を消費する第２の手段はダミー信号線を有することを特徴とする請求項１、２のいずれかに記載の情報処理装置。

【請求項１６】前記第２の電力を消費する第２の手段はダミー信号線を有することを特徴とする請求項１、２のいずれかに記載の情報処理装置。

【請求項１７】　第１のデータ処理装置と、第２のデータ処理装置と、この両者を接続する信号線と、プリチャージ信号の制御手段と、前記信号線で消費される第１の電力と、当該信号線での電力消費とは別の第２の電力を消費する手段とを少くなくとも有し、前記第１あるいは第２のデータ処理装置は前記第２の電力を消費する手段に接続され、且つ前記第２あるいは第１のデータ処理装置は前記プリチャージ信号の制御手段に接続され、前記第１と第２のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第１の電力消費と前記第２の電力消費の和が所定値となされるごとく構成されたことを特徴とする情報処理装置。

【請求項１８】　第１のデータ処理装置と、第２のデータ処理装置と、これらを接続する信号線と前記信号線をプリチャージするためのプリチャージ信号線制御装置を少なくとも有し、前記第１のデータ処理装置は、前記プリチャージ信号線制御装置に接続され、さらに相補的プリチャージバス制御装置にも接続され、前記プリチャージバス制御装置は、前記信号線に接続され、前記相補的プリチャージバス制御装置は前記信号線での第１の電力消費とは別の第２の電力を消費する手段に接続され、前記データ信号線での第１の消費電力と前記第２の消費電力の和が所定値になるように、前記信号線のプリチャージ直後にバスに流すデータをビット反転して第２の電力を消費する手段に入力されることを有することを特徴とする情報処理装置。

【請求項１９】　前記第２の電力を消費する第２の手段はプリチャージダミー信号線を有することを特徴とする請求項１７または１８のいずれかに記載の情報処理装置。

【請求項２０】　第１のデータ処理装置と、第２のデータ処理装置と、これらをつなぐ信号線と、前記信号線をプリチャージするプリチャージ信号線制御手段とを少なくとも有し、前記信号線は、当該信号線の途中に反転装置を少なくとも有

し、当該反転装置を挟んで、正論理と負論理との信号線から構成されることを特徴とする情報処理装置。

【請求項２１】　信号の暗号化に用いる鍵情報を自動的に設定することが可能なことを特徴とする請求項７に記載の情報処理装置。

【請求項２２】　信号の暗号化の鍵情報の一部として、情報処理装置の有する記憶情報の番地情報を用いて暗号化あるいは復号化がなされる事を特徴とする請求項７に記載の情報処理装置。

【請求項２３】　信号の暗号化の鍵情報を設定あるいは変更する手段を有する暗号化あるいは複号化がなされる事を特徴とする請求項７に記載の情報処理装置。

【請求項２４】　信号の暗号化に用いた鍵情報及び複号化に必要な暗号情報を記憶する領域を有するデータ処理装置と、当該データ処理装置内に記憶された暗号情報に基づいて複号化がなされる事を特徴とする請求項７に記載の情報処理装置。

【請求項２５】　信号の暗号化あるいは複号化が、記憶装置を複数の領域に分割し、領域ごとに暗号化の有無を指定するための暗号化領域指定手段を有し、暗号化するか否かを記憶装置の領域に応じて指定可能な事を特徴とする請求項７に記載の情報処理装置。

【請求項２６】　信号の暗号化あるいは複号化が、特定のデータパタンに対しては暗号化を行わない事を特徴とする請求項７に記載の情報処理装置。

【請求項２７】　信号の暗号化に用いる鍵情報を自動的に設定が可能な事を特徴とする請求項８に記載の情報処理装置。

【請求項２８】　信号の暗号化の鍵情報の一部として、記憶装置の番地情報を用いて暗号化あるいは復号化をなす事を特徴とする請求項８に記載の情報処理装置。

【請求項２９】　信号の暗号化に用いる鍵情報を定期的に自動再設定が可能な事を特徴とする請求項８に記載の情報処理装置。

【請求項３０】　信号の暗号化あるいは複号化に対しての暗号化の鍵情報を設定あるいは変更が可能なことを特徴とする請求項８に記載の情報処理装置。

【請求項３１】　データ処理装置と情報記憶装置と、これらを結ぶ信号線を少なくとも有し、前記データ処理装置と前記信号線の間で暗号化が可能であり、前記信号線と前記情報記憶装置との間で複号化が可能なことを特徴とする情報処理装置。

【請求項３２】　信号の暗号化に用いる鍵情報を自動的に設定が可能なことを特徴とする請求項３１に記載の情報処理装置。

【請求項３３】　暗号化に用いる鍵情報を定期的に自動再設定が可能なことを特徴とする請求項３１に記載の情報処理装置。

【請求項３４】　信号の暗号化あるいは複号化に対しての暗号化の鍵情報を設定あるいは変更が可能なことを特徴とする請求項３１に記載の情報処理装置。

【請求項３５】　複数の情報を格納可能で、格納された複数の情報の格納場所を番地によって区別して、記録あるいは読み出しが可能であり、情報を格納する際に情報を暗号化し、情報を読み出す際の複号化が可能なことを特徴とする情報記憶装置。

【請求項３６】　信号の暗号化の鍵情報の一部として、記憶装置の番地情報を用いる事を特徴とした請求項３５に記載の情報記憶装置。

【請求項３７】　信号の暗号化鍵を自動的に初期化することが可能なこと特徴とする請求項３５に記載の情報記憶装置。

【請求項３８】　信号の暗号化を行う記憶領域を指定する暗号化領域指定レジスタと、暗号化領域指定レジスタの値と、番地情報を参照して、暗号化暗号化を行うか否かの判定を行い、特定の記憶領域の情報のみを暗号化することを可能とする、暗号化領域判定装置を有する事を特徴とする請求項３５に記載の情報記憶装置。

【請求項３９】　信号の暗号化の鍵情報の一部として、記憶装置の番地情報を用いる事を特徴とする請求項９に記載の情報記憶装置。

【請求項４０】　信号の暗号化を行う記憶領域を指定する暗号化領域指定レジスタと、暗号化領域指定レジスタの値と、番地情報を参照して、暗号化を行うか否かの判定を行い、特定の記憶領域の情報のみを暗号化することを可能とする事を特徴とする請求項９に記載の情報記憶装置。

【請求項４１】　記憶装置と、記憶装置を含むデータ処理装置と、それらを結ぶ信号線と、記憶装置と記憶装置を含むデータ処理装置との間の情報転送を制御する情報転送制御装置装置とを少なくとも有し、前記情報転送制御装置装置が、転送元の情報が格納された番地を記憶するためのアドレスレジスタと、転送先の番地を記憶するためのアドレスレジスタと、転送する情報の数をカウントするための数値を格納するカウンタと、カウンタの値をデクリメントするための演算回路と、記憶装置間で転送するデータを一時的に保存するデータバッファと、アドレスレジスタの値を更新するための演算回路と、転送アドレスの転送順番をランダム化する回路を有することを特徴とする情報処理装置。

【請求項４２】　情報処理装置と、当該第１の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とするカード部材。

【請求項４３】　端末機と、前記端末機に接続可能なカード部材とを少なくとも有し、前記カード部材は、情報処理装置と、当該第１の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とする情報処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本願発明は、高いセキュリティを持つ情報処理装置および情報記憶装置に関するものである。更には、本願発明は、カード部材および情報処理システムに関するものである。当該カード部材としては、特にＩＣカード（スマートカード）に代表される、１チップのＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）を情報処理装置として内蔵するものをあげることが出来る。

【０００２】

【従来の技術】

ＩＣカードに代表される高いセキュリティを持ったマイクロコンピュータチッ

プでは、勝手に書き換えられない情報の保持や秘密情報である暗号鍵を使って秘匿すべきデータの暗号化や暗号文の復号化を行うことがある。

【０００３】

マイクロコンピュータの基本構成は、図１に示すように、中央演算装置８００１、記憶装置８００２、そして各部の情報のやりとりを行うための道である信号線８００３を有している。中央処理装置８００１は、論理演算や算術演算などを行う装置であり、記憶装置８００２は、プログラムやデータを格納する装置である。記憶装置８００２は、例えばＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）やＲＡＭ（Ｒａｎｄｕｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲｅａｄＯｎｌｙ Ｍｅｍｏｒｙ）、ＦＲＡＭ（Ｆｅｒｒｏｍａｇｎｅｔｉｃ Ｒａｎｄｕｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）などを用いて構成される。ＲＯＭは、変更できないメモリであり、主にプログラムを格納するメモリである。ＲＡＭは自由に書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消去される。従ってデバイスに電源の供給が中断されると、ＲＡＭの内容は、保持できなくなる。ＥＥＰＲＯＭ、ＦＲＡＭは、電源の供給が中断されてもその内容を保持することができるメモリである。

【０００４】

例えば接触型ＩＣカードに供されるコンピュータの本体の例を、図２に示す。図２にはこの半導体装置のチップ５１の端子配置のみを示している。当該コンピュータの本体は、カードの中央の横に配置されたＣＯＴと呼ばれるチップである。図２には端子配置の例が示されている。即ち、ＩＣカードは、Ｖｃｃ（供給電源）、ＧＮＤ（グランド）、ＲＳＴ（リセット）、Ｉ／Ｏ（入出力）、およびＣＬＫ（クロック）の端子を持つ。前記チップはこれらの信号を外部から、即ち、例えば端末機から、供給されることによって稼動する。尚、前記端末機自体は基本的に通例のカード・システムのものを用いて十分である。この場合、消費電力はＶｃｃとＧＮＤとの信号を観察することによって測定することができる。この消費電力の測定については、Ｊｏｈｎ Ｗｉｌｅｙ ＆ ｓｏｎｓ社、Ｗ. Ｒａｎｋｌ Ｗ. Ｅｆｆｉｎｇ著１９９７年「Ｓｍａｒｔ Ｃａｒｄ Ｈａｎｂｏｏｋ

」の8.5.1.1 Passive protective mechanisms（２６３ページ）に記載されている。

【０００５】

【発明が解決しようとする課題】

本願発明の課題は、高いセキュリティを持つ情報処理装置を提供せんとするものである。当該情報処理装置としてはコンピュータシステム、わけてもマイクロコンピュータシステムを代表例としてあげることが出来る。

【０００６】

更には、本願発明は、高いセキュリティを持つ、ＩＣカード（スマートカード）に代表されるカード部材、およびカード・システムを提供するものである。

【０００７】

本願発明のより技術的な課題を示せば、それは、マイクロコンピュータチップでのデータ処理と消費電力との関連性を減少させることである。特にＩＣカードは、重要な情報を格納したり、カードの中で暗号処理を行うために用いられている。それは、プログラムや重要な情報がＩＣカード用チップの中に密閉されているためである。ＩＣカードでの暗号の解読は、暗号に対するアルゴリズムの解読の困難さと同程度と考えられていた。しかし、ＩＣカードが暗号処理を行っている際の消費電力を観測し、この消費電力の状態を解析することにより、暗号処理の内容や暗号鍵が推定される可能性が示唆されている。この消費電力を観測する方法は、暗号に対するアルゴリズムの直接的な解読する方法よりも容易であると目されている。

【０００８】

従って、消費電力とチップの処理との関連性が薄れれば、観測した消費電力の波形からＩＣカードチップ内での処理や暗号鍵の推測が困難になる。本願発明の着眼点は、マイクロコンピュータの消費電力と処理されるデータとの関連を減少させることである。その手段の主なものは、消費電力の差を生み出す原因の一つである信号線（例えば、バスラインや、ＲＡＭ内のビット線、ワード線等）の充放電を均一にするか、又は、元のデータと異なるものにすることによるものである。

【０００９】

以下にまず、本願発明の背景となる消費電力の観測による、処理信の解読の可能性について説明する。このことが理解されれば、本願発明の趣旨が容易に理解されよう。

【００１０】

上述の消費電力の測定の骨子は次の通りである。ＩＣカード用チップの有するＣＭＯＳ（Ｃｏｍｐｌｅｍｅｔａｒｙ Ｍｅｔａｌ－Ｏｘｉｄｅ－Ｓｅｍｉｃｏｎｄｕｃｔｏｒ）のゲート回路は、出力状態が１から０あるいは０から１に変わった時に電力を消費する。特に信号線は大きな配線容量を持つため、当該ゲート回路は、バスのデータ値が１から０あるいは０から１に変わると、その充放電のために大きな電力を消費する。そのため、こうした消費電力を観測すれば、ＩＣカード用チップの中での情報処理の内容が解読される可能性がある。

【００１１】

図３は、ＩＣカード用チップの１サイクルでの消費電力の波形を示したものである。処理している諸データの値に依存して、消費電力の諸波形が１１０１や１１０２のように異なる。このような複数の消費電力に対する波形の差は、信号線を流れるデータや中央演算装置で処理しているデータ等に依存して生じる。

【００１２】

現在、ＩＣカード用チップの信号線の制御方式には、大別して二つの種類がある。一つはスタティック信号線制御方式であり、もう一つがプリチャージ信号線制御方式である。

【００１３】

スタティック信号線制御方式は、バスに乗っているデータのクリアは行わないものである。一方、プリチャージ信号線制御方式は、一回の処理が終わる毎にデータをクリアするために、信号線のデータを全て１または０にしてから次のデータを乗せる制御方式である。尚、プリチャージを信号値の１か０のどちらにするかは、論理回路が順論理か、逆論理かで異なる。しかし、その動作の本質は変わらない。

【００１４】

上述の基本動作の説明から明らかなように、この制御方式の違いにより、消費電力の波形が異なる。消費電力波形の違いから、どちらの制御方式を用いているかを判断する事ができる。

【００１５】

信号線の制御方式がわかれば、暗号鍵は決まっているため、処理するデータを変更して、消費電力を観測することにより、暗号鍵のビット値の影響が観測できる可能性が生ずる。また、これらの消費電力の波形を分析することにより、暗号鍵を推定できる可能性が生ずる。

【００１６】

【課題を解決するための手段】

本願発明の基本となる考え方をまず説明し、次いで、本願に開示される主な発明の諸形態を列挙する。本願発明の基本となる考え方は大きくは次の４つの方法に大別される。

【００１７】

＜１．信号線の電力の消費の均一化＞

第１の方法は、例えば情報処理装置における、例えばメモリの駆動方式やデータ内容に基づく消費電力の差を減少させる方法である。具体的には、この方法は、マイクロコンピュータ内部の信号線での電力の消費の他にも、例えば簡単には、前記信号線での電力消費に対応して、これとは別に充放電装置にて電力の消費を行うことによって、伝達される各信号列毎の消費電力の差を減少させるものである。

【００１８】

＜２．信号線内のデータの暗号化＞

第２の方法は、例えば情報処理装置において、信号線にのせるデータを暗号化し、当該信号線での電力消費を撹乱する方法である。即ち、この方法は、マイクロコンピュータ内部の信号線にデータを乗せる際に、データの暗号化を行い、データを受信する装置に入力する際にこのデータの復号化を行うものである。こうして、前記信号線での電力消費を撹乱することが出来る。

【００１９】

＜３．記憶情報の暗号化＞

第３の方法は、例えば情報処理装置において、暗号化したデータを記憶部に格納する方法である。即ち、この方法は、例えばマイクロコンピュータの記憶装置に暗号化したデータを格納し、このデータの演算等を行う際に復号化して利用することにより、信号線での電力消費を撹乱するものである。

【００２０】

＜４．データ転送順序の交換＞

第４の方法は、例えば情報処理装置において、データ転送順序を変更する方法である。即ち、マイクロコンピュータの記憶装置に格納されているデータを信号線に載せて転送する際に、転送の順序を入れ替えることにより、信号線での電力消費を撹乱するものである。

【００２１】

尚、必要に応じて、上記４つの発明の形態を組み合わせて、併用することが出来る。また、このような諸形態の併用によって、より有効に半導体装置の高セキュリティを確保することが出来る。この併用の諸例を例示すれば次のごとき方法である。

【００２２】

それらは、（１）信号線の電力の消費を均一化しつつ信号線内データの暗号化する方法、（２）信号線の電力の消費を均一化しつつ記憶情報の暗号化を図る方法、（３）電力の消費の均一化を図りつつデータ転送順序の交換する方法、（４）信号線内データの暗号化しつつ記憶情報の暗号化を図る方法、（５）信号線内データの暗号化しつつデータ転送順序の交換する方法、（６）記憶情報の暗号化を図りつつデータ転送順序の交換する方法である。

【００２３】

更に、２つ以上の方法を併用することも可能である。即ち、それらは（７）信号線内データの暗号化しつつ信号線の電力の消費の均一化を図り、且つ記憶情報の暗号化を図る方法、（８）信号線内データの暗号化しつつ信号線の電力の消費の均一化を図り、且つデータ転送順序の交換する方法、（９）信号線内データの

暗号化しつつ記憶情報の暗号化を図り且つデータ転送順序の交換する方法、（１０）記憶情報の暗号化を図りつつデータ転送順序の交換し且つ信号線の電力の消費の均一化する方法である。更には、それは（１１）信号線の電力の消費の均一化、信号線内データの暗号化、記憶情報の暗号化、およびデータ転送順序の交換する方法である。

【００２４】

以下、前記の４つの基本形態を柱として、それぞれの諸形態について詳細に説明する。

【００２５】

（１）信号線の電力の消費の均一化

本願の発明思想の第１は、前述の通り、例えば、メモリの駆動方式やデータ内容に基づく消費電力の差を減少させる方法である。

【００２６】

この方法は、先に例示したマイクロコンピュータ内部の信号線での電力の消費の他にも、前記信号線でのディジタル・データの転送に伴う電力消費に対応する電力の消費を行なわせる手段、例えば簡単には、電荷の充放電する手段、装置を設けるものである。この充放電装置によって、前記信号線でのディジタル・データの転送に伴う電力消費に対応する電力を消費させ、上記伝達信号列によらずその消費電力の差を減少させるものである。即ち、当該マイクロコンピュータにおける信号線で消費される電力と、充放電装置において消費される電力の和を同一にするのである。各記憶装置の信号線に対する両消費電力の和が常に同一であれば、仮にデバイスの消費電力のデータが取り出せても、内部情報を知る事は非常に困難となる。

【００２７】

尚、以下、電荷の充放電する手段、装置を単に充放電装置と称する。以下に説明するように、当該充放電装置として、例えばダミーデータ線を用いて構成することも出来る。

【００２８】

本願発明に係わる一例では、上述の考え方に基づき、マイクロコンピュータ内

部の２つのデータ処理装置を接続している信号線を介してデータの転送を行う際、このデータのディジタル信号に応じて、ビットを反転して充放電装置に入力し、当該信号線で消費される電力と、当該充放電装置で消費される電力の両者を同一にする。制御信号発生装置が発生する信号に応じて、定常消費電流発生装置を作動させることにより、当該信号線に乗せるデータを、充放電装置での消費電力と当該信号線で消費される電力が常に一定になるように、マイクロコンピュータチップの消費電力と処理しているデータの関連を減少させる。

【００２９】

尚、前記２つのデータ処理装置は、具体的には、例えば、ＲＯＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＲＡＭ、ＦＲＡＭ等を有して構成されている。

【００３０】

以下、信号線の制御方式の相違への対応を含めて本形態を説明する。即ち、入力されるビットデータは、信号線の制御方式によって異なる。

【００３１】

いわゆる、ＣＭＯＳ回路では、ビット反転、すなわち、データが０から１または、１から０に変化する時、特に電力が消費される。このように、信号線では、ビット反転が起きるときに消費電力が大きくなる。従って、本願発明では、当該記憶装置に設けた充放電装置によって、前記ビット反転の回数に応じて充放電装置でも同様の電力消費を行うようにする。こうして、信号線で消費される電力と、充放電装置で消費される電力の両者の和が一定になり、信号線を流れるデータとマイクロコンピュータチップの消費電力との関連性を緩和する事ができる。

【００３２】

信号線におけるビット反転個数は、信号線の制御方式によってことなる。信号線の制御方式は、前述の通り、スタッティック信号線制御方式とプリチャージ信号線制御方式とがある。その各々について説明する。

【００３３】

まず、スタティック信号線制御方式の場合を考える。この場合、データはクリアされず、前のデータが信号線に残っている。実際の装置では、信号線は実質的に、コンデンサと同じ機能を持っている。従って、ここで前述の「残っている」

というのは、物理的には、電荷が残っているという意味である。従って、前に信号線に乗っていたデータの値を記憶しておけば、次に乗るデータに応じて、消費電力がどのように変わるかがわかる。

【００３４】

この消費電力と充放電装置で消費される電力を同一にするためには、信号線で電力消費が行われるときには充放電装置に入力するデータは変化させず、信号線で電力消費が行われないときには、充放電装置に入力するデータを変化させ、両者の消費電力の合計が、常に一定になるようにする。この場合、消費電力は、内部処理のうち信号線を介さないものの消費電力を除いて、単一の信号線において常にビット反転が起こっている状態と同一になり、内部処理データと無関係となるため、内部処理データと消費電力の関連性を減少させることができる。

【００３５】

一方、プリチャージ信号線制御方式においては、データの転送毎にデータが毎回クリアされる。従って、信号線での消費電力は、信号線に直前に乗っていたデータによらず、次に乗るデータを二進法表示したときに現れる１の個数に比例する。尚、逆論理なら信号線での消費電力は０の個数に比例する。

【００３６】

従って、プリチャージ信号線制御方式の場合に、この消費電力と充放電装置で消費される電力を同一にするためには、データを信号線に乗せると同時に、このデータのビット反転値分を充放電装置に流す事である。こうして、信号線で消費される電力と、充放電装置で消費される電力の両者の消費電力の合計が、常に一定になるようにする。この場合も、マイクロコンピュータの消費電力は、内部処理のうち信号線を介さないものの消費電力を除いて、単一の信号線において常にビット反転が起こっている状態と同一になり、内部処理データと無関係となるため、内部処理データと消費電力の関連性を減少させることができる。

【００３７】

多くのマイクロコンピュータチップの内部では、スタティック信号線制御方式と、プリチャージ信号線制御方式とが混在している。従って、マイクロコンピュータチップ全体の消費電力変化と処理データとの関連性を減少させるには、前述

の両方法を用いた情報処理装置を合わせて用いる必要がある。

【００３８】

（２）信号線に乗せるデータの暗号化

次に、信号線に乗せるデータを暗号化する方法について説明する。この方法によれば、信号線での消費電力は、実際のデータに基づく消費電力とは別のものになっている。従って、仮に、半導体装置より消費電力のデータが取り出せても、半導体装置の内部情報を知る事は困難となる。

【００３９】

本発明の形態では、マイクロコンピュータ内部の２つのデータ処理装置（ＲＯＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＲＡＭ、ＦＲＡＭ等を有して構成されている）を接続している信号線を介してデータの転送を行う際、データを転送する側は定められた暗号化方式によって暗号化を行う暗号化装置によって暗号化したデータを転送する。一方、データを受信する装置は、この暗号化されたデータを復号化する復号化装置によって当該暗号化データを復号して処理を行う。このような処理によれば、信号線は元のデータと異なるデータによる充放電を行うので、内部処理データと消費電力の関連性を減少させることができる。この方法による効果は、信号線の制御方式がスタティック方式であるかプリチャージ方式であるかにかかわらず期待することができる。

【００４０】

（３）記憶情報の暗号化

第３は、記憶装置に記憶させるデータを暗号化して格納する方法である。この方法は、例えば、読み出し専用のメモリであるＲＯＭにデータを書き込む際に定められた暗号化方式によってデータを暗号化してから格納する。このデータをデータ処理装置等で利用する際には、この暗号化されたデータを定められた方式によって復号化する復号化装置によって復号してからデータ処理装置に入力する。この方法では、信号線に乗る転送データは、暗号化されたデータとなり、信号線は元のデータと異なるデータによる充放電を行うので、内部処理データと消費電力の関連性を減少させることができる。この方法による効果は、信号線の制御方式がスタティック方式であるかプリチャージ方式であるかにかかわらず期待する

ことができる。

【００４１】

（４）データ転送順序の交換

第４は、信号線に乗せるデータの転送順序を元とは異なるものにする方法である。この方法は、例えば、転送するデータが、毎クロックおきに、Ａ、Ｂ、Ｃ、Ｄ、Ｅの順序で転送されるところを、Ｅ、Ａ、Ｂ、Ｄ、Ｃの順序で転送する。このデータの転送順序は勿論一例である。この方法により、信号線の充放電のパターンは、本来の順序通りに行われない。従って、信号線は元のデータと異なるデータによる充放電を行うので、内部処理データと消費電力の関連性を減少させることができる。この方法の効果は、信号線の制御方式がスタティック方式であるかプリチャージ方式であるかにかかわらず期待することができる。

【００４２】

以下に本願発明の主な諸形態を列挙する。

【００４３】

本願発明の第１の形態は、情報処理装置と、当該第１の情報処理装置につながれた信号線とを有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とする情報処理装置である。

【００４４】

第２の形態は、第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線とを有し、前記第１もしくは第２の情報処理装置の少なくとも一方よりの信号を伝達する前記信号線での第１の電力の消費状態に対応して第２の電力の消費状態が定められ、且つ前記信号線での第１の電力の消費と前記第２の電力の消費とが互いに相反する期間に可能とされていることを特徴とする情報処理装置である。

【００４５】

第３の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置の信号を伝達する前記信号線での第１の電力の消費状態に対応して第２の電力の消費状態が定められ、且つ前記信号線での第１の電力の消

費と前記第２の電力の消費との和が所望値となされるごとく構成されたことを特徴とする情報処理装置である。

【００４６】

第４の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置の信号を伝達する前記信号線での第１の電力の消費状態に対応して第２の電力の消費状態が定められ、且つ前記信号線での第１の電力の消費がなされる期間では、前記第２の電力の消費がなされず、前記信号線での第１の電力の消費がなされない期間では第２の電力の消費が可能とされていることを特徴とする情報処理装置である。

【００４７】

第５の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置のディジタル信号を伝達する前記信号線での信号値の反転に対応して電力の消費が可能とされていることを特徴とする情報処理装置である。

【００４８】

第６の形態は、第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線と、前記第１もしくは第２の情報処理装置の少なくとも一方よりのディジタル信号に基づく前記信号線での第１の電力の消費状態に対応して、前記信号線での転送信号の信号値の反転に対応して第２の電力の消費がなされる手段を有することを特徴とする情報処理装置である。

【００４９】

第７の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置と前記信号線との間において、前記情報処理装置よりの信号を暗号化が可能であり且つ前記信号線より暗号化されて転送される信号を復号化することが可能なことを特徴とする情報処理装置である。

【００５０】

第８の形態は、第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線とを有し、前記第１の情報処理装置あるいは第２の情報処理装置の少なくとも１者と前記信号線との間において、前記第１の情報処理装置あるいは第２

の情報処理装置よりの信号を暗号化し、且つ前記信号線より転送されてくる信号を復号化することが可能なことを特徴とする情報処理装置である。

【００５１】

第９の形態は、第１の情報処理装置と、第２の情報処理装置と、その両者を結ぶ信号線とを有し、前記第１の情報処理装置よりの信号を暗号化し、当該暗号化された第１の情報処理装置よりの信号を復号化して第２の情報処理装置に入力し、且つ前記第２の情報処理装置の出力を暗号化し、当該暗号化された第２の情報処理装置よりの信号を復号化して第１の情報処理装置に入力することが可能なことを特徴とする情報処理装置である。

【００５２】

第１０の形態は、情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報の復号化が可能なことを特徴とする情報処理装置である。

【００５３】

第１１の形態は、情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報を復号化して、前記信号線を介して前記情報処理装置に入力が可能なことを特徴とする情報処理装置である。

【００５４】

第１２の形態は、情報処理装置と、当該情報処理装置につながれた信号線とを有し、前記情報処理装置よりの出力される信号列が、その順序を異にして前記信号線を伝達され、且つ前記信号列の異にされた順序を復元が可能なことを特徴とする情報処理装置である。

【００５５】

第１３の形態は、情報処理装置と、当該第１の情報処理装置につながれた信号線とを有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていること

を特徴とするカード部材である。

【００５６】

尚、本願は、それらの列挙は避けるが、ここに掲げた例以外に、前記の諸情報処理装置あるいは前記の諸情報記憶装置を有する諸カード部材を提供出来るものである。更には、本願は、後述する情報処理装置あるいは前記の諸情報記憶装置を有する諸カード部材を提供出来るものである。

【００５７】

第１４の形態は、端末機と、前記端末機に接続可能なカード部材とを少なくとも有し、前記カード部材は、情報処理装置と、当該第１の情報処理装置につながれた信号線とを有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされていることを特徴とするカード・システムである。

【００５８】

尚、本願は、その列挙は避けるが、ここの掲げた例以外に、前記情報処理装置あるいは前記情報記憶装置を有する諸カード・システムを提供出来るものである。更には、本願は、後述する情報処理装置あるいは前記の諸情報記憶装置を有する諸カード・システムを提供出来るものである。

【００５９】

加えて、本願発明の更なる諸形態を列挙する。これらによって、本願発明の諸形態をより具体的に理解されるであろう。

【００６０】

第１５の形態は、二つのデータ処理装置Ａ、Ｂとこれらを接続する信号線（制御信号によってバスラインのデータをクリアしない制御方式で制御される信号線：スタティック信号線）と、制御信号発生装置を有するマイクロコンピュータにおいて、該データ処理装置Ａ、Ｂ間において該信号線を介して情報の転送を行う際、該信号線で消費される電力と、充放電装置で消費される電力の和が一定になるように、制御信号発生装置からの信号に応じて、データ処理装置Ａから出力されたデータ（ＤＡＴＡ）と、直前に該信号線に乗っているデータ（ＰＢＤ）と、直前に充放電装置に入力されたデータ（ＣＤＤ）に対して、以下の表１にしたが

って、充放電装置への入力を行い、信号線には、データ処理装置Ａから出力されたデータ（ＤＡＴＡ）を入力する為に該データ処理装置Ａに接続された電力発生装置Ｃを有することを特徴とする情報処理装置である。

【００６１】

【表１】

PBD	DATA	CDD	本願の充放電装置への出力
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

表１

【００６２】

尚、ここで、理解を容易とする為、本願明細書において、「電力発生装置」との用語を用いるが、これは、前述したように、信号線での電力の消費の他にも、前記信号線でのデータの転送に伴う電力消費に対応する電力の消費を行なわせる手段である。即ち、上記用語における「電力発生」とは信号線の電力の消費を均一化し、伝送する信号列によらず、基本的に同じ電力の消費を行うとの意味である。この装置が一般的に「電力を発生する」意でないことを注記して置く。

【００６３】

第１６の形態は、二つのデータ処理装置Ａ、Ｂとこれらを接続する信号線（制御信号によってバスラインのデータをクリアしない制御方式で制御される信号線

：スタティック信号線）と、制御信号発生装置を有するマイクロコンピュータにおいて、該データ処理装置Ａ、Ｂ間において該信号線を介して情報の転送を行う際、該信号線で消費される電力と、充放電装置で消費される電力の和が一定になるように、制御信号発生装置からの信号に応じて、データ処理装置Ａから出力されたデータ（ＤＡＴＡ）と、直前に該信号線に乗っているデータ（ＰＢＤ）と、直前に充放電装置に入力されたデータ（ＣＤＤ）に対して、上記の表１にしたがって、充放電装置への入力を行い、信号線には、データ処理装置Ａから出力されたデータ（ＤＡＴＡ）を入力する為に該データ処理装置Ａ、Ｂそれぞれに接続された電力発生装置Ｃ、Ｄ（ＣとＤが同一である場合を含む）を有することを特徴とする情報処理装置である。

【００６４】

第１７の形態は、第１のデータ処理装置と、第２のデータ処理装置と、この両者を接続する信号線と、プリチャージ信号の制御手段と、前記信号線で消費される第１の電力と、当該信号線での電力消費とは別の第２の電力を消費する手段とを少くなくとも有し、前記第１あるいは第２のデータ処理装置は前記第２の電力を消費する手段に接続され、且つ前記第２あるいは第１のデータ処理装置は前記プリチャージ信号の制御手段に接続され、前記第１と第２のデータ処理装置間において前記信号線を介して信号の転送を行う際、前記第１の電力消費と前記第２の電力消費の和が所定値となされるごとく構成されたことを特徴とする情報処理装置である。

【００６５】

第１８の形態は、データ処理装置Ａと、データ処理装置Ｂと、これらを接続する信号線と該信号線をプリチャージするためのプリチャージ信号線制御装置を有するマイクロコンピュータにおいて、該データ記憶装置は、該プリチャージ信号線制御装置に接続され、さらに相補的プリチャージバス制御装置にも接続され、該プリチャージバス制御装置は、該データ信号線に接続され、該相補的プリチャージバス制御装置は、充放電装置に接続され、該データ信号線での消費電力と、該充放電装置で消費される電力の和が一定になるように該データ信号線のプリチャージ直後にバスに流すデータをビット反転して該充放電装置に入力する該相補

的プリチャージバス制御装置を有することを特徴とする情報処理装置である。

【００６６】

第１９の形態は、二つのデータ処理装置Ａ、Ｂと、これらを接続する信号線と該信号線をプリチャージするプリチャージ信号線制御装置とを有する情報処理装置において、信号線の途中に反転装置を有し、反転装置を挟んで、同一の配線容量を持つ正論理と負論理の信号線から構成される信号線を有することを特徴とする情報処理装置である。

【００６７】

第２０の形態は、データ処理装置Ａとデータ処理装置Ｂとこれらを結ぶ信号線とを有する情報処理装置において、信号線とデータ処理装置Ｂのデータを暗号化するための暗号化装置、復号化装置をデータ処理装置Ａと信号線との間に有する事を特徴とする情報処理装置である。

【００６８】

第２１の形態は、データ処理装置Ａとデータ処理装置Ｂとこれらを結ぶ信号線を有する情報処理装置において、信号線とデータ処理装置Ｂ内のデータを暗号化・復号化するための暗号化・復号化装置をデータ処理装置Ａと信号線との間およびデータ処理装置Ｂと信号線の間に有する事を特徴とする情報処理装置である。

【００６９】

以下は、わけても本願の情報記憶装置に関する主な発明の諸形態である。

【００７０】

第２１の形態は、データ処理装置と情報記憶装置と、これらを結ぶ信号線を有する情報処理装置において、データ処理装置と信号線の間に暗号化装置を有し、信号線と情報記憶装置との間に複号化装置を有することを特徴とした、情報処理装置である。

【００７１】

第２２の形態は、複数の情報を格納可能で、格納された複数の情報の格納場所を番地によって区別し、記録・読み出しが可能な情報記憶装置において、情報を格納する際に情報を暗号化する暗号化装置と、情報を読み出す際の複号化装置とを有する事を特徴とする情報記憶装置である。

【００７２】

第２３の形態は、データ処理装置と、情報をあらかじめ暗号化して記憶している情報記憶装置と、情報記憶装置とデータ処理装置を結ぶ信号線と、暗号化された情報を複号化する複号化装置とを有することを特徴とした、情報処理装置である。

【００７３】

第２４の形態は、記憶装置と、記憶装置を含むデータ処理装置と、それらを結ぶ信号線に接続され、記憶装置と記憶装置を含むデータ処理装置との間の情報転送を制御する情報転送制御装置装置において、転送元の情報が格納された番地を記憶するためのアドレスレジスタと、転送先の番地を記憶するためのアドレスレジスタと、転送する情報の数をカウントするための数値を格納するカウンタと、カウンタの値をデクリメントするための演算回路と、記憶装置間で転送するデータを一時的に保存するデータバッファと、アドレスレジスタの値を更新するための演算回路と、転送アドレスの転送順番をランダム化する回路を有することを特徴とする情報転送制御装置である。

【００７４】

以上、本願発明の関する主な発明の諸形態を説明したが、更に、本願発明においては、前記充放電装置として、データを配送する信号線と同等の配線容量を持つダミー信号線を有することものを用いることが出来る。更には、前記充放電装置として、データを配送する信号線と同等のプリチャージダミー信号線を有するものを用いることが出来る。

【００７５】

また、鍵情報を用いる形態は、起動時に暗号化に用いる鍵情報を自動的に設定する暗号化キー自動設定装置を用いることが出来る。あるいは、鍵情報を用いる形態は、暗号化に用いる鍵情報を定期的に自動再設定する暗号化キー自動再設定装置を用いることが出来る。

【００７６】

また、暗号化の鍵情報の一部として、記憶装置の番地情報を用いる暗号化・復号化装置を用いることが出来る。更には、暗号化複号化装置として、暗号化の鍵

情報を設定・変更する手段を有する暗号化複号化装置としても良い。

【００７７】

また、本願発明の情報処理装置は、暗号化に用いた鍵情報及び暗号化の方式などの複号化に必要な暗号情報を記憶する領域を有するデータ処理装置Ｂと、データ処理装置Ｂ内に記憶された暗号情報に基づいて複号化を行う複号化装置を用いて構成することが出来る。また、暗号化・複号化装置として、記憶装置を複数の領域に分割し、領域ごとに暗号化の有無を指定するための暗号化領域指定装置を有し、暗号化するか否かを記憶装置の領域に応じて指定可能な暗号化・複号化装置を用いて構成することが出来る。また、暗号化・複号化装置として、特定のデータパタンに対しては暗号化を行わない暗号化・複号化装置を用いて構成することが出来る。

【００７８】

また、本願発明の情報処理装置は、起動時に暗号化に用いる鍵情報を自動的に設定する暗号化キー自動設定装置を用いて構成することが出来る。更には、暗号化に用いる鍵情報を定期的に自動再設定する暗号化キー自動再設定装置をを用いて構成することが出来る。

【００７９】

また、本願発明の情報処理装置は、複数の情報を格納可能で、格納された複数の情報の格納場所を番地によって区別し、記録・読み出しが可能な情報記憶装置において、情報を格納する際に情報を暗号化する暗号化装置と、情報を読み出す際の複号化装置とを用いることが出来る。更には、暗号化・復号化装置の暗号化鍵を自動的に初期化する暗号化鍵自動設定装置を用いることが出来る。また、本願発明の情報処理装置は、暗号化を行う記憶領域を指定する暗号化領域指定レジスタと、暗号化領域指定レジスタの値と、番地情報を参照して、暗号化暗号化を行うか否かの判定を行い、特定の記憶領域の情報のみを暗号化することを可能とする暗号化領域判定装置を用いることが出来る。

【００８０】

【発明の実施の形態】

図５は発明の第１の実施の形態を説明する為の情報処理装置の概要を説明する

基本構成図である。勿論、図５は情報処理装置の当該発明に係わる部分の主要部のみを例示している。当該情報処理装置の他の部分は通例の構成を用いて十分である。

【００８１】

本実施の形態の例の情報処理装置は、データ処理装置Ａ（ＲＯＭ）０１０１(Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ：リード・オンリー・メモリ)とデータ処理装置Ｂ(ＣＰＵ)０１０２(Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ:中央処理装置)とが信号線（バスライン）０１１３にて接続されている。そして、情報処理装置Ａ側に電力発生装置Ｃ ０１１４が設けられている。

【００８２】

この電力発生装置Ｃの例は、排他的論理和演算装置(ＥＸＯＲ)０１０３、０１０４、インバータ０１０５、ＰＭＯＳゲート回路０１０７、ＮＭＯＳゲート回路０１０８、抵抗器Ｒ０１０９、コンデンサＣ ０１１０、データの一時記憶用のラッチ回路（フリップフロップ）などを有して図のように構成されている。尚、リード・オンリー・メモリはデータ読み出し専用のメモリで、データの書き込みはできない。データの一時記憶用のラッチ回路は０１１１、０１１２を有して構成されている。

【００８３】

尚、ここでデータ処理装置（ＲＯＭ）等の表示は、ＲＯＭを主として構成したデータ処理装置を意味している。他の情報処理装置（ＲＡＭ）も同様である。

【００８４】

また、この例において、抵抗器Ｒ ０１０９の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサＣ０１１０の静電容量は、信号線の信号容量に等しいものとする。ここでは説明を簡単にするため、信号線のサイズは１ビットとし、ＣＰＵは８ビットプロセッサであるものとする。尚、信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【００８５】

まず、本願発明を用いない通例の半導体記憶装置では、信号線を介する消費電

力の観測から、半導体装置の内部情報をいかに推定できるのかを説明する。この説明によって本願発明の有効性が十分に理解されるであろう。

【００８６】

データ処理装置Ａ（ＲＯＭ）　０１０１内に記憶されているデータをデータ処理装置Ｂ(ＣＰＵ)０１０２に転送する場合、これを信号線（バスライン）０１１３に乗せて転送しなければならない。

【００８７】

ここに、信号線（バスライン）０１１３のデータ転送に要する消費電力を観測する観測者がいた場合、当該観測者は、本願発明に係わる電力発生装置Ｃがなければ、次のような事実を観測することが出来る。即ち、データが、仮に「０１０００１０１００１」という並びだったとすると、０から１、１から０にビット反転するときに発生する消費電力を観測することにより、「反転、反転、未反転、未反転、反転、反転、反転、反転、未反転、反転」という事がわかる。

【００８８】

この消費電力の観測結果に基づく「反転と未反転」のデータ列は、当該データ列の直前のデータビットの値によって次の２つの状態であることが判明する。即ち、前記データの直前のデータビットの値が不明である場合、次の２つの状態である。

【００８９】

（１）直前のデータが０と仮定した場合、当該データ列は０１０００１０１００１であることになる。

【００９０】

（２）直前のデータが１と仮定した場合、当該データ列は１０１１１０１０１１０であることになる。

【００９１】

このように、消費電力の観測による分析は、本来は２の１２乗、即ち４０９６通りあるデータ列が、僅か上記の２通りにまで減少する。従って、極めて多く存在する情報の可能性がわずか２つの可能性まで推測され、従って、存在するのが僅か２つの可能性であれば、その可能性より内部情報を十分把握することが可能

となる。

【００９２】

本願発明はこうした消費電力の分析を阻止するひとつの方策を提供するものである。

【００９３】

尚、ここで、本願発明の情報処理装置の動作の説明をするに先立って、本願発明に係わる電力発生装置の例について説明する。勿論、例示する電力発生装置以外にも具体的構成を考えることは可能である。以下に事例についても同様である。

【００９４】

図５で点線で囲った部分０１１５は、本電力発生装置の論理演算を行う回路領域を示す。符号０２０３と０２０４は排他的論理和を行う回路である。符号０２０５は反転回路で、「０」の入力に対しては「１」を出力する回路である。

【００９５】

この回路の論理式表示は、次のようになる。

【００９６】

Ｒ＝ｎｏｔ（ＣＤＤ　ｅｘｏｒ　（ＰＢＤ　ｅｘｏｒ　ＤＡＴＡ））

この論理式の出力は前述の表１の如くになる。このことは、排他的論理和（ｅｘｏｒ）が表２となることから、容易に理解出来る。

【００９７】

尚、ここで、ＣＤＤは考察するデータ信号の直前に、充放電装置に入力されたデータ、ＰＢＤは考察するデータ信号の直前に、当該信号線に乗っているデータ、更にＤＡＴＡはデータ処理装置Ａから出力されたデータである。

【００９８】

【表２】

X	Y	X exor Y
0	0	0
1	0	1
0	1	1
1	1	0

表２

【００９９】

又、ＰＢＤあるいはＣＤＤのデータの一時記憶方法として、図６に例示するフリップフロップをあげることが出来る。ここで、ＮＡＮＤ（９０２、９０３、９０４、９０５）は、表３に従って出力する演算装置である。ＮＯＴ（９０１）はビットを反転する装置で、図４におけるビット反転回路と同じものである。

【０１００】

【表３】

X	NOT X
0	1
1	0

表３

【０１０１】

図６にデータの一時記憶用のフリップフロップ回路は、制御信号が１の時、ＰＢＤはバスのデータを出力し、制御信号が０のとき、ＰＢＤはそれ以前の値を保つ。本フリップフロップ回路のより具体的な使用形態は後述される。

【０１０２】

実際、制御信号をＣＳ（Ｃｏｎｔｒｏｌ　Ｓｉｇｎａｌ）、バスラインのデータをＢＵＳと表示するならば、このフリップフロップ回路の動作は、次の４つの論理式で表すことが出来る。

【０１０３】

ｘ＝ＢＵＳ　ｎａｎｄ　ＣＳ

ｙ＝（ｎｏｔ　ＢＵＳ）　ｎａｎｄ　ＣＳ

ＰＢＤ＝ｘ　ｎａｎｄ　ＰＢＤ

ｚ＝ｙ　ｎａｎｄ　ＰＢＤ

今、制御信号ＣＳが１であるとすると、ｎａｎｄはビットを反転するから、上述の論理式は次の通りとなる。

【０１０４】

ｘ＝ｎｏｔ　ＢＵＳ

ｙ＝ＢＵＳ

ｚ＝ｙ　ｎａｎｄ　ＰＢＤ

ＰＢＤ＝ｘ　ｎａｎｄ　ｚ

従って、ＢＵＳが１であれば、０　ｎａｎｄ　ｚ＝１より、ＰＢＤ＝１となる。ＢＵＳが０であれば、ｚ＝０　ｎａｎｄ　ＰＢＤ＝１、ＰＢＤ＝（ｎｏｔＢＵＳ）　ｎａｎｄ　１＝ＢＵＳ＝０となる。こうして、ＰＢＤはＢＵＳと一致する。

【０１０５】

一方、制御信号が０の時は、ｘもｙも１であるから、ＰＢＤは前の値を保持する。

【０１０６】

＜本願発明の第１の実施の形態での動作＞

次に本例の情報処理装置における、データ転送の処理を、図１を参酌して、具体的に説明する。

【０１０７】

ＲＯＭ０１０１からプログラムの一部である命令［ＥＸＯＲ　Ｒ２、Ｒ４］が信

号線０１１３を通してＣＰＵに転送される場合を考える。これが、１６進数で、［ＣＡ ２４］という機械語に対応するものとする。このデータは信号線に流される際、１１００１０１０００１０００１００というビットパターンとなる。

【０１０８】

先ず、次の初期条件を仮定して考察する。第１にこのデータの直前に信号線に乗ったデータが０であると仮定する。また、第２に定常消費電力発生装置Ｃのコンデンサは、充電状態にあるとする。即ち、この状態はデータ１が乗っている状態に対応する。更に、第３にＣＰＵからデータがバスに乗ったということを知らせる制御信号が、ラッチ０１１１、０１１２に入力されるものとする。

【０１０９】

[（１）信号列の最初の「１」の転送＝データ「０」より「１」の変換動作]

まず、最初の１が乗る際に、信号線０１１３は充電され、当該信号線０１１３に１が乗っている状態となる。このとき、同じデータが定常消費電力発生装置Ｃ０１１４に入力される。このとき、電力発生装置Ｃ０１１４がどのように動作するかを詳細に説明する。

【０１１０】

ＣＰＵからのデータ１は排他的論理和演算装置０１０３に入力される。同時に、ＣＰＵからデータの出力信号を受けて、ラッチ回路０１１２は、保持していた信号線０１１３に直前に乗っていた値０を排他的論理演算装置０１０３に入力する。このとき、排他的論理演算装置０１０３は、以下の前述の表２にしたがって演算を行うので、０と１の排他的論理和は１となる。この値が、排他的論理和演算装置０１０４に入力される。

【０１１１】

ＣＰＵからのデータの出力信号を受けて、ラッチ回路０１１１は、保持しているコンデンサ０１１０のデータ（電荷）１を排他的論理和演算装置０１０４に入力するので、排他的論理和演算装置０１０４は、表２にしたがって、０を出力する。この値は、インバータ０１０５に入力され、前述の表３にしたがって値１を出力する。

【０１１２】

この１という値が、ＰＭＯＳゲート０１０７に入力される。ＰＭＯＳは、ゲート電圧がＬＯＷのときのみ通電するので、この場合は通電しない。一方、インバータ０１０５から出力された値１は、ＮＭＯＳゲート０１０８に入力されている。これにより、ゲート０１０８が通電し、コンデンサ０１１１が放電を行う。これによって信号線０１１３とコンデンサ０１１１における電力消費量の和は信号線を１本充電したときと同じになる。

【０１１３】

［（２）データが「１」より「１」への変換動作］

次のデータは、１で、直前の信号線０１１３のデータも１である。コンデンサは充電状態である。このときの定常消費電力発生装置の動作は以下のようになる。

【０１１４】

まず、情報処理装置Ｂ（ＣＰＵ）０１０２からのデータ１が乗る際は、信号線０１１３は既に充電状態にあり、信号線０１１３は充電されない。このとき、同じデータが定常消費電力発生装置Ｃ０１１４に入力される。情報処理装置Ｂ（ＣＰＵ）０１０２からのデータ１は排他的論理和演算装置０１０４に入力される。同時に、情報処理装置Ｂ（ＣＰＵ）０１０２からデータの出力信号を受けて、ラッチ回路０１１２は、保持していた信号線０１１３に直前に乗っていた値１を排他的論理演算装置０１０３に入力する。このとき、排他的論理演算装置０１０３は、表２にしたがって演算を行うので、１と１の排他的論理和は、０となる。この値が、排他的論理和演算装置０１０４に入力される。

【０１１５】

情報処理装置Ｂ（ＣＰＵ）０１０２からのデータの出力信号を受けて、ラッチ回路０１１１は、保持しているコンデンサ０１１０のデータ（電荷）１を排他的論理和演算装置０１０４に入力するので、排他的論理和演算装置０１０４は、表２にしたがって、１を出力する。この値は、インバータ０１０５に入力され、表３にしたがって値０を出力する。

【０１１６】

この０という値が、ＰＭＯＳゲート０１０７に入力される。このＰＭＯＳは、ゲート電圧がＬｏｗのときのみ通電する。従って、この場合は通電状態になり、Ｖｄｄが供給され、コンデンサ０１１０が充電される。一方、インバータ０１０５から出力された値０は、ＮＭＯＳゲート０１０８に入力されている。これにより、このＮＭＯＳゲート０１０８が通電しない。ここでコンデンサ０１１０は１ビット分の電力を消費し、これによって信号線０１１３とコンデンサ０１１０における電力消費量の和は信号線を１本充電したときと同じになる。

【０１１７】

［（３）データが「１」より「０」への変換動作］

次のデータは、０である。信号線０１１３のデータは１であり、コンデンサ０１１０は放電した状態にある。このときの電力発生装置０１１４の動作は次のようになる。

【０１１８】

まず、情報処理装置Ｂ（ＣＰＵ）０１０２からのデータ０が乗る際は、信号線０１１３は充電状態にあるので、信号線０１１３では放電が行われる。信号線０１１３上の電荷は放電によって１ビット分の電力を消費する。このとき、同じデータ０が定常消費電力発生装置Ｃ０１１４に入力される。情報処理装置Ｂ（ＣＰＵ）０１０２からのデータ０は排他的論理和演算装置０１０３に入力される。同時に、情報処理装置Ｂ（ＣＰＵ）０１０２からデータの出力信号を受けて、ラッチ回路０１１２は、保持していた信号線０１１３に直前に乗っていた値１を排他的論理演算装置０１０３に入力する。このとき、排他的論理演算装置０１０３は、表２にしたがって演算を行うので、０と１の排他的論理和は、１となる。この値が、排他的論理和演算装置０１０４に入力される。

【０１１９】

情報処理装置Ｂ（ＣＰＵ）０１０２からのデータの出力信号を受けて、ラッチ回路０１１１は、保持しているコンデンサ０１１０のデータ（電荷）０を排他的論理和演算装置０１０４に入力するので、排他的論理和演算装置０１０４は、表２にしたがって、１を出力する。この値は、インバータ０１０５に入力され、表

３にしたがって値０を出力する。

【０１２０】

この０という値が、ＰＭＯＳゲート０１０７に入力される。このＰＭＯＳは、ゲート電圧がＬｏｗのときのみ通電する。従って、この場合は通電状態になり、Ｖｄｄが供給され、コンデンサ０１１０の充電が行われる。一方、インバータ０１０５から出力された値０は、ＮＭＯＳゲート０１０８に入力されている。これにより、このＮＭＯＳゲート０１０８が通電しない。これによって信号線０１１３とコンデンサ０１１０における電力消費量の和は信号線を１本充電したときと同じになる。

【０１２１】

以下、全く同様の流れで、表１の全ての場合を導くことができる。図７の（ｂ）は、先の命令コード「１１００１０１０００１００１００」に対するデータの流れとコンデンサの状態を示している。

【０１２２】

このようにして、全てのパターンについて、信号線０１１３とコンデンサ０１１０の消費電力の和は、信号線０１１３の１ビット充放電において消費される電力と同じである。従って、デバイスの消費電力を調べることによって信号線０１１３に乗ったデータを推測することが困難となる。

【０１２３】

こうして製造された情報処理装置を内蔵する半導体集積回路装置を、カード部材に適用して、高セキュリティのカード部材を提供することが出来る。カード部材における半導体集積回路装置のの配置は、図２に示したものと基本的に同様である。カード部材としては接触型と非接触型があるが、本願発明はいずれの方式にも当然適用することが出来る。

【０１２４】

そして、前記チップはこれらの信号を外部から、即ち、例えば端末機から、供給されることによって稼動する。

【０１２５】

尚、前記端末機自体は基本的に通例のカード・システムのものを用いて十分で

ある。以下、簡単にカード・システムの動作を例示する。図３はこのカード・システムの概念を例示する。

【０１２６】

ＩＣカード５２の中にはチップ５１があって、リーダライタ５３とデータのやりとりを行う例を示している。リーダライタのなかには、コントロールプロセッサ５４およびデータベースとなる磁気ディスク５５などが存在する。まず、リーダライタ５３からＩＣカード５２に対して、ＩＤの問い合わせが行われる。まず、リーダライタ５３からＩＣカード５２に対して、ＩＤ（ＩＤＥＮＴＩＦＩＣＡＴＩＯＮ）、例えば、当該カードの管理責任者を特定する為の氏名コードまたは認識コードの問い合わせが行われる。図３にはこの状態を（１）として示した。この氏名コードまたは認識コードはＩＣチップの中にある所定のエリアに格納されている。 ＩＣカードは氏名コードをリーダライタに返答する。図３にはこの状態を（２）として示した。リーダライタはデータベース５３にある氏名コードを検索して、データベース上の鍵コードを獲得する。

【０１２７】

リーダライタは乱数をＩＣカードに送る。この乱数は、例えばリーダライタ内のＭＰＵで回路的に発生される。ＬＡＮ等でサーバ側から乱数を供給することも出来る。ＩＣカードは、乱数を受け取った時点で、コマンドによってリーダライタから指示を受け、乱数を鍵コード発生部に従って発生した鍵コードによって暗号化した乱数を作成する。

【０１２８】

一方、リーダライタはＩＣカードと同様にデータベースから得た鍵コードを使用して、ＩＣカードへ送ったのと同じ乱数を暗号化する。これによって得られた暗号化された乱数の結果と先のＩＣカードからの暗号化された乱数を照合して、一致がとれれば、ＩＣカードとリーダライタの相互認識が完了して、ＩＣカードの正当性が認められる。

【０１２９】

このようにして、本システムでは、この鍵コードがリーダライタに伝えられるとリーダライタは磁気ディスクの中のＩＤを検索して、正しく登録された鍵コー

ドによるＩＤであると認識する。

【０１３０】

生成されたＩＣカードの鍵コード（ＩＤコード）は、氏名コードまたは認識コードとともにデータベースに格納される。

【０１３１】

生成された鍵コードは電子マネーとしてＩＣカードが使用される時の本人認証や偽造チェックやＩＣカードとリーダライタの相互認証に使用することが出来る。

【０１３２】

上記システムは、例えば、一般商店での支払や、チケットの購入、定期券での改札、免許証のチェック、テレフォンカードによる電話等々多くの分野に応用することが出来る。

【０１３３】

以上のようなカード部材ならびにカード・システムは、以下に述べる発明の諸形態を用いて実施可能なことは言うまでもない。

【０１３４】

続いて、本願発明に係わる情報処理装置の実施の諸形態を説明する。

【０１３５】

図８は発明の第２の実施の形態を説明する為の情報処理装置の概要の基本構成図である。本例は、情報処理装置間の信号の伝達が双方向に行われ、且つ電力発生装置を双方の情報処理装置に共有して設けられた例である。

【０１３６】

本実施例の情報処理装置では、情報処理装置Ａ（ＣＰＵ）０２０１と情報処理装置Ｂ(ＲＡＭ) ０２０２(Ｐａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ:データの読み書きができるメモリ)とが信号線（バスライン）０２１３によってつながれている。そして、情報処理装置Ａ（ＣＰＵ）０２０１と情報処理装置Ｂ(ＲＡＭ)０２０２に対して電力発生装置Ｃ０１１４が設けられている。

【０１３７】

電力発生装置Ｃ０１１４は、排他的論理和演算装置(ＥＸＯＲ)０２０３、０２

０４、インバータ０２０５、ＮＭＯＳゲート回路０２０７、ＰＭＯＳゲート回路０２０８、抵抗器Ｒ０２０９、コンデンサＣ　０２１０、データの一時記憶用のラッチ回路（フリップフロップ）０２１１、０２１２を有する。ここで、抵抗器Ｒ０２０９の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサＣ０２１０の静電容量は、信号線の信号容量に等しいものとする。ここでは簡単のため、信号線のサイズは１ビットとし、ＣＰＵは８ビットプロセッサであるものとする。尚、信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分である。

【０１３８】

本実施の形態においては、前述の情報処理装置の第１の実施の形態の構成を一部そのまま用いている。特に、情報処理装置Ａ（ＣＰＵ）０２０１から、情報処理装置Ｂ（ＲＡＭ）０２０２にデータを信号線０２１３によって転送する場合は、第１の実施の形態の情報処理装置の例におけるＲＯＭから、ＲＡＭにデータを転送する際の定常消費電力発生装置の動作と全く同じ動作を行う。

【０１３９】

本例において特徴的なのは、情報処理装置間の信号の伝達が双方向に行われることである。即ち、それは、第１の実施の形態の情報処理装置の例のように一方的なデータ転送ではなく、情報処理装置Ａ（ＣＰＵ）０２０１から情報処理装置Ｂ（ＲＡＭ）０２０２へのデータ転送だけでなく、情報処理装置Ｂ（ＲＡＭ）０２０２から情報処理装置Ａ（ＣＰＵ）０２０１へのデータ転送も行うということである。

【０１４０】

従って、これに伴って定常消費電力発生装置０１１４が、その双方のデータ転送に際してその機能を果たすように接続されている。

【０１４１】

本例においては、情報処理装置Ａ（ＣＰＵ）０２０１が、情報処理装置Ｂ（ＲＡＭ）０２０２に対してデータの読み出し信号を送り、それを受けて情報処理装置Ｂ（ＲＡＭ）０２０２がデータを信号線０２１３に乗せると同時に、排他的論理和演算装置０２０３にもデータを送信する。これ以後の動作は、第１の実施の形態の情報処理装置の例において、情報処理装置Ａ（ＲＯＭ）０１０１から、情報処

理装置Ｂ（ＣＰＵ）０１０２にデータを転送する際の定常消費電力発生装置０１１４の動作と全く同じである。従って、その動作の詳細説明は省略する。

【０１４２】

図８においては、情報処理装置Ａ(ＣＰＵ)０２０１と定常消費電力発生装置Ｃ０１１４との距離が、情報処理装置Ｂ(ＲＡＭ)０２０２と定常消費電力発生装置Ｃ０１１４との間の距離よりも短く図示されている。しかし、実際の構成では、ほぼ同じ距離に位置させ、情報処理装置Ａ(ＣＰＵ)０２０１あるいは情報処理装置Ｂ(ＣＰＵ)０２０２と定常消費電力発生装置Ｃ０１１４とのデータのやりとりを行う信号線は、情報処理装置Ａ(ＣＰＵ)０２０１あるいは情報処理装置Ｂ(ＣＰＵ)０２０２と信号線０２１３との間の信号線よりも短いものとする。このとき、消費電力を調べることによっては、信号線０２１３に乗ったデータを推測することが困難となる。

【０１４３】

図９は発明の第２の実施の形態の変形例を説明する為の情報処理装置の基本構成図である。本例は、情報処理装置間の信号の伝達が双方向に行われ、且つ電力発生装置が双方の情報処理装置に対応して設けられた例である。

【０１４４】

本実施例の情報処理装置は、情報処理装置Ａ（ＣＰＵ）０２５１、情報処理装置Ｂ(ＲＡＭ）０２５２が信号線（バスライン）０２６３によってつながれている。そして、前記双方の情報処理装置に対して電力発生装置Ｃ０１１５、および電力発生装置Ｄ０１１６が配されている。

【０１４５】

電力発生装置Ｃ０１１５は、排他的論理和演算装置(ＥＸＯＲ)０２５３、０２５４、インバータ０２５５、ＰＭＯＳゲート回路０２５７、ＮＭＯＳゲート回路０２５８、抵抗器Ｒ ０２５９、コンデンサＣ０２６０、データの一時記憶用のラッチ回路（フリップフロップ）０２６１、０２６２を有して構成される。電力発生装置Ｄは、排他的論理和演算装置(ＥＸＯＲ)０２６４、０２６５、インバータ ０２６６、ＰＭＯＳゲート回路０２６８、ＮＭＯＳゲート回路０２６９、抵抗器Ｒ０２７０、コンデンサＣ０２７１、データの一時記憶用のラッチ回路（フ

リップフロップ）０２７２、０２７３を有して構成される。

【０１４６】

次に、次の条件を仮定してその動作を考察する。抵抗器Ｒ０２５９の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサＣ０２６０の静電容量は、信号線の信号容量に等しいものとする。

【０１４７】

ここでは簡単のため、信号線のサイズは１ビットとし、ＣＰＵは８ビットプロセッサであるものとする。尚、信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分である。

【０１４８】

本例においては、第１の実施の形態の情報処理装置の例の構成を一部そのまま用いている。特に、情報処理装置Ａ（ＣＰＵ）０２５１から、情報処理装置Ｂ（ＲＡＭ）０２５２にデータを信号線０２６３によって転送する場合は、第１の実施の形態の情報処理装置の例において、情報処理装置Ａ（ＲＯＭ）０１０１から、情報処理装置Ｂ（ＣＰＵ）０１０２にデータを転送する際の定常消費電力発生装置の動作と全く同じ動作を行う。従って、その詳細説明は省略する。

【０１４９】

本例で特徴的なのは、第１の実施の形態における情報処理装置の実施例のように一方的なデータ転送ではなく、情報処理装置間の信号の伝達が双方向に行われることである。即ち、この例では、情報処理装置Ａ（ＣＰＵ）０２５１から情報処理装置Ｂ（ＲＡＭ）０２５２へのデータ転送だけでなく、情報処理装置Ｂ（ＲＡＭ）０２５２から情報処理装置Ａ（ＣＰＵ）０２５１へのデータ転送も行う。本実施例においては、情報処理装置Ａ（ＣＰＵ）０２５１が、情報処理装置Ｂ（ＲＡＭ）０２５２に対してデータの読み出し信号を送り、それを受けて情報処理装置Ｂ（ＲＡＭ）０２５２がデータを信号線０２６３に乗せると同時に、定常消費電力発生装置Ｄ０１１６における、排他的論理和演算装置０２６４にもデータを送信する。定常消費電力発生装置Ｄ０１１６は、定常消費電力発生装置Ｃ０１１５と同一のものである。そして、これ以後の動作は、第１の実施の形態における情報処理装

置の実施例において、情報処理装置Ａ（ＲＯＭ）０１０１から、情報処理装置Ｂ（ＣＰＵ）０１０２にデータを転送する際の定常消費電力発生装置の動作と全く同じである。このとき、消費電力を調べることによって信号線０２６３に乗ったデータを推測することが困難となる。

【０１５０】

図１０は発明の第３の実施の形態を説明する為の情報処理装置の基本構成図である。

【０１５１】

本実施例の基本的構造は、第１の実施の形態と同様である。本例は、ダミー信号線を用いる例である。即ち、本例では、第１の実施の形態に例示した抵抗器０１０９とコンデンサ０１１０の部分が、ダミー信号線０３０９に置き換えられている。

【０１５２】

本実施例の情報処理装置は、データ処理装置Ａ（ＲＯＭ）０３０１とデータ処理装置Ｂ（ＣＰＵ）０３０２とが信号線（バスライン）０３１２でつながれている。そして、データ処理装置Ａ（ＲＯＭ）０３０１に対して、電力発生装置Ｃ０１１７が設けられている。電力発生装置Ｃ０１１７は、排他的論理和演算装置（ＥＸＯＲ）０３０３、０３０４、インバータ０３０５、ＰＭＯＳゲート回路０３０７、ＮＭＯＳゲート回路０３０８、ダミー信号線０３０９、データの一時記憶用のラッチ回路（フリップフロップ）０３１０、０３１１を有して構成される。

【０１５３】

ここで、ダミー信号線０３０９の静電容量は、信号線０３１２の静電容量に等しいものとし、抵抗値は、信号線０３１２のそれと実質的に同じであるものとする。即ち、ダミー信号線０３０９は信号線０３１２と全く同一の信号線を用いると考えてよい。ここでは説明を簡単にのため、信号線のサイズは１ビットとし、ＣＰＵは８ビットプロセッサであるものとする。尚、信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０１５４】

本例では、前記ダミー信号線０３０９の静電容量が、第１の実施の形態に例示した抵抗器０１０９とコンデンサ０１１０の部分と同等の役割を果たす。従って、本例の動作は基本的に第１の実施の形態における情報処理装置の実施の形態と同様である。従って、その詳細説明は省略する。

【０１５５】

図１１は発明の第４の実施の形態を説明する為の情報処理装置の基本構成図である。本例はプリチャージ信号線制御方式であって、且つ電力発生装置を有する例である。

【０１５６】

本実施例の情報処理装置は、データ処理装置Ａ（ＲＯＭ）０４０１とデータ処理装置Ｂ（ＣＰＵ）０４０２が信号線０４０８によってつながれている。そして、電力発生装置Ｃ０１１８がデータ処理装置Ａ（ＲＯＭ）０４０１側に設けられている。そして、本例は、プリチャージ方式の制御であるので、プリチャージ信号線制御装置０４０７を有している。

【０１５７】

プリチャージ信号線制御装置０４０７は、二つのＰＭＯＳゲート回路０４０９、０４１０を有し、そのゲート部には、データ処理装置Ｂ（ＣＰＵ）０４０２からのデータ制御信号が入力される。ソース側には、Ｖｄｄが接続されており、データ処理装置Ｂ（ＣＰＵ）０４０２からの制御信号に応じて信号線０４０８及び電力発生装置Ｃ０１１８にＶｄｄを供給する。電力発生装置Ｃ０１１８は、ＮＭＯＳゲート回路０４０４、抵抗器（Ｒ）０４０５、コンデンサＣ０４０６、論理積演算回路０４１１を有する。ここで、抵抗器Ｒ０４０５の抵抗値は、信号線の抵抗値に等しいものとし、コンデンサＣ　０４０６の静電容量は、信号線の信号容量に等しいものとする。ここでは説明を簡単にのため、信号線のサイズは１ビットであるものとし、ＣＰＵは８ビットプロセッサであるとする。信号線のサイズは、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０１５８】

データ処理装置Ａ（ＲＯＭ）０４０１内に記憶されているデータをデータ処理装置Ｂ（ＣＰＵ）０４０２に転送する場合、データ信号を信号線（バスライン）０４０８に乗せて転送しなければならない。

【０１５９】

ここで、信号線（バスライン）０４０８のデータ転送に要する消費電力を観測する観測者がいた場合を考えてみる。今、データが、仮に「０１０００１０１００１」という並びだったとする。そして、定常電力発生装置Ｃ０１１８がない場合、プリチャージ信号線制御装置０４０７の働きによって、前記のデータ値が０から１に変化するときに発生する消費電力を観測することにより、このデータ列が、「０１０００１０１００１」であることが直接わかる。尚、ここでは、正論理で考えるものとした。すなわち、信号線の電位がＬＯＷのとき、データ値は、０であり、ＨＩＧＨのときにデータ値１に対応する。勿論、負論理の場合にも同じようにデータ値が１から０に変化するときに発生する消費電力を観測することにより、データ列を推測することが出来る。

【０１６０】

本願発明はこうした消費電力の分析を阻止するひとつの方策を提供するものである。本例のデータ転送の処理は次の通りである。

【０１６１】

ＲＯＭ０４０１からプログラムの一部である命令［ＥＸＯＲ Ｒ２、Ｒ４］が信号線０４０８を通してデータ処理装置Ｂ（ＣＰＵ）０４０２に転送される場合を考える。これが、１６進数で、［ＣＡ ２４］という機械語に対応するものとする。このデータは信号線に流される際、「１１００１０１０００１００１００」というビットパターンとなる。

【０１６２】

データ処理装置Ｂ（ＣＰＵ）０４０２が制御信号を発信すると、プリチャージ信号線制御装置０４０７の二つのＰＭＯＳ０４０９、０４１０のゲートが通電してＶｄｄを信号線０４０８に供給して１（ＨＩＧＨ）にクリアする。更に、当該電位は、電力発生装置Ｃ０１１８のコンデンサ０４０６を充電する。まず、最初

のデータ（ＭＤ－ＤＡＴＡ）１が乗る際に、信号線の放電が行われ、電力が消費される。このとき、同じデータ（ＭＤ－ＤＡＴＡ）１とＭＡＣＫ信号が電力発生装置Ｃ０１１８に入力される。

【０１６３】

このとき、定常電力発生装置Ｃ０１１８がどのように動作するかを詳細に述べる。

【０１６４】

前記のデータ列の最初の値「１」の場合、データ処理装置Ａ（ＲＯＭ）０４０１からのデータ（ＭＤ－ＤＡＴＡ）１が準備される。この最初の値「１」の準備によって、データ処理装置Ａ（ＲＯＭ）０４０１はＭＡＣＫ信号を出力する。ＭＡＣＫ信号は、出力が確定すると１であり、確定していない状態では０となる。ＭＡＣＫ信号が論理積演算装置０４１１に入力され、同時にデータ（ＭＤ－ＤＡＴＡ）１が、信号線０４０８に乗る。そして、さらに、データ（ＭＤ－ＤＡＴＡ）１は論理積演算装置０４１１に入力される。

【０１６５】

ＭＤ－ＤＡＴＡ、ＭＡＣＫ信号が共に１であるから、論理積演算装置０４１１の出力は１である。そして、この値は、ＮＭＯＳゲート回路０４０４に入力される。ＮＭＯＳゲート回路０４０４は、入力１（ＨＩＧＨ）に対しては通電するので、コンデンサ０４０６は放電を行う。一方、信号線０４０８上の値は変化しないので、信号線０４０８での充放電は行われない。

【０１６６】

充放電を行なわない信号線０４０８においては電力消費はなく、一方、放電を行なうコンデンサ０４０６では電力の消費がなされる。従って、その両者の和は、信号線１本の充電で消費される消費電力に等しい。

【０１６７】

次に、前記のデータ列の第２の値「１」の場合、データ１が信号線０４０７に乗る。このときには既に信号線０４０７はプリチャージされ１にクリアされているので、再び上で説明したのと同じ動作が行われ、信号線０４０８における消費電力と、コンデンサ０４０６における消費電力の和は、信号線一本の充電で消費

される消費電力に等しい。

【０１６８】

次に、前記のデータ列の第３の値「０」の場合、データ（ＭＤ－ＤＡＴＡ）０が信号線０４０８に乗る。このときは、既に信号線０４０８はプリチャージされ１にクリアされているので、値「１」から「０」への変化に伴って電力消費が行われる。ＭＤ－ＤＡＴＡ０とＭＡＣＫ信号１は、論理積演算装置０４１１に入力される。論理積演算装置０４１１の出力値は０となり、この値は、ＮＭＯＳゲート回路０４０４に入力される。ＮＭＯＳゲート回路０４０４は、入力０（ＬＯＷ）に対しては通電しないので、コンデンサ０４０６での電力消費は行われない。

【０１６９】

データ値「１」から「０」への変化がある前記信号線では電力の消費があり、一方、コンデンサ０４０６では電力の消費がない。従って、その両者の消費電力の和は、信号線１本の充電で消費される消費電力に等しい。

【０１７０】

以下同様の動作を行うので、常に信号線０４０８における消費電力と、コンデンサ０４０６における消費電力の和は、信号線一本の充電で消費される消費電力に等しい。

【０１７１】

上述の信号線０４０８でのデータ「１１００１０１０００１００１００」に対するコンデンサ０４０６の状態を、相互に対応させて図７の（ａ）に示す。

【０１７２】

図１２は発明の第５の実施の形態を説明する為の情報処理装置の基本構成図である。本例はプリチャージ信号線制御方式であって、且つ電力発生装置としていわゆるダミー信号線を用いた例である。

【０１７３】

本実施例の基本的構造は、第４の実施の形態と同様であって、抵抗器とコンデンサの部分が、ダミー信号線に置き換えられただけである。本実施例の情報処理装置は、データ処理装置Ａ（ＲＯＭ）０５０１、データ処理装置Ｂ（ＣＰＵ）０５０２、プリチャージ信号線制御装置０５０５、信号線（バスライン）０５０６

、定常電力発生装置Ｃ０１１９を有する。ここで、ダミー信号線０５０７の静電容量は、信号線０５０６の静電容量に等しいものとし、抵抗値は、信号線０５０６のそれと同じであるものとする。即ち、ダミー信号線 ０５０７と信号線０５０６とは実質的に同一の信号線を用いる。尚、定常電力発生装置Ｃ０１１９は、ＮＭＯＳゲート回路０５０４、ダミー信号線０５０７、 論理積演算装置０５０３を有する。

【０１７４】

ここでは簡単のため、信号線のサイズは１ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０１７５】

動作は基本的に前述の第１の実施の形態の情報処理装置の実施例と同様である。従って、その詳細説明は省略する。

【０１７６】

図１３は発明の第６の実施の形態を説明する為の情報処理装置の基本構成図である。本例はプリチャージ信号線制御方式であって、且つ反転装置を有する例である。

【０１７７】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）５００１とデータ処理装置Ｂ（ＲＡＭ）５００２とが、各々信号線５００７、５００６につながれている。そして、両信号線５００７と５００６の間に反転装置５００３が設けられている。更に、本例はプリチャージ信号線制御装置５００８を有する。

【０１７８】

反転装置５００３は、４つのＣＭＯＳインバータ５００４、５００５、５００９、５０１０、ＰＭＯＳゲート回路５０１１、５０１３、ＮＭＯＳゲート回路５０１４、５０１２を有して構成されている。尚、信号線５００６と信号線５００７の静電容量並びに抵抗値は実質的に同一であるものとする。

【０１７９】

データ処理装置Ａ（ＣＰＵ）５００１から、データ処理装置Ｂ（ＲＡＭ）５００２にデータを転送する際、データ処理装置Ａ（ＣＰＵ）５００１は、制御信号をプリチャージバス制御装置５００８に発信する。この信号によって、プリチャージバス制御装置５００８内のＰＭＯＳゲート及びＮＭＯＳゲートを通電する。そして、電位Ｖｄｄが信号線 ５００７、５００６を充電してＨＩＧＨの状態にする。更に、データ処理装置Ａ（ＣＰＵ）５００１からの制御信号がインバータ５０１０、ＮＭＯＳゲート回路５０１２に入力され、ＰＭＯＳゲート回路５０１１、ＮＭＯＳゲート回路５０１２が通電状態になる。この後、データ処理装置Ａ（ＣＰＵ）５００１からデータが送信される。

【０１８０】

データ処理装置Ａ（ＣＰＵ）５００１からのデータが０のとき、信号線５００７が放電する。この値はインバータ５００４によって１に変換され、信号線５００６に信号を送る。しかし、前述の通り、既に信号線５００６は充電されているので充放電は起きない。そして、この値１がデータ処理装置Ｂ（ＲＡＭ）５００２に入力される。この値「１」は、データ処理装置Ａ（ＣＰＵ）５００１が送ったデータ「０」とは反転している。

【０１８１】

逆にデータ処理装置Ａ（ＣＰＵ）５００１からのデータが、１であった場合は、信号線５００７では充放電が起きず、信号線５００６で放電が生ずる。データ処理装置Ｂ（ＲＡＭ）５００２からデータ処理装置Ａ（ＣＰＵ）５００１にデータが送られる場合も同様である。信号線５００６と信号線５００７の静電容量並びに抵抗値は実質的に同一であるから、全ての場合において、信号線５００６、５００７での充放電の総和は信号線５００６あるいは５００７の充放電で生ずる電力が消費され、総和は一定となる。

【０１８２】

次に、第７の実施の形態より第２２の実施の形態の諸形態は、信号線に乗せるデータを暗号化する諸例である。

【０１８３】

図１４は発明の第７の実施の形態を説明する為の情報処理装置の基本構成図である。本例は暗号化装置を用いて信号線に乗せるデータの暗号化を図る基本的な例である。

【０１８４】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）０６０１とデータ処理装置Ｂ（ＲＡＭ）０６０２とが信号線（バスライン）０６０５によってつながれている。そして、データ処理装置Ａ（ＣＰＵ）０６０１と信号線（バスライン）０６０５との間に暗号化装置および復号化装置を有する。本例の暗号化装置としては排他的論理和演算装置０６０３及び、復号化装置としては排他的論理和演算装置０６０４が用いられている。尚、こうした暗号化装置および復号化装置として他の構成の諸装置を用いることが出来ることは言うまでもない。

【０１８５】

ここでは説明を容易にするのため、信号線０６０５のサイズは８ビットとし、データ処理装置Ａ（ＣＰＵ）０６０１は８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

又、ここでは、信号線０６０５の制御方式はスタティック信号線制御方式であるとして説明する。尚、本実施の形態の思想の効果は、プリチャージ信号線制御方式においても同じである。

【０１８６】

本例の暗号化装置は、固定された８ビットの鍵（Ｋｅｙ）とＣＰＵからの８ビットのデータとのビット毎の排他的論理演算装置である。一方、本例の復号化装置も同じ鍵とデータとのビット毎の排他的論理和演算装置である。尚、鍵（Ｋｅｙ）自体は通例の技術で十分である。

【０１８７】

第１の発明の実施の形態の実施例で述べたように、スタティック信号線制御方式の場合は、信号線に直前に乗っていた値とのビット反転数に比例して電力消費が行われる。以下、１ビットに対する消費電力をＰと表示する。

【０１８８】

例えば、データ処理装置Ａ（ＣＰＵ）０６０１からデータ「０１１０１００」を送信したとする。信号線０６０５に直前に乗っていたデータが、「１１０１０１０１」であるとすると、ビット反転数は５である。従って、この信号線０６０５で消費される電力は５Ｐである。

【０１８９】

データ処理装置Ａ（ＣＰＵ）０６０１から、データ「１０１１０１１１」を信号線０６０５を通してデータ処理装置Ｂ（ＲＡＭ）０６０２に転送し、これを再び、データ処理装置Ｂ（ＲＡＭ）０６０２よりデータ処理装置Ａ（ＣＰＵ）０６０１に戻す過程を考える。この場合、信号線０６０５に直前に乗っていたデータは、「００００１０１０１」であると仮定する。又、鍵（Ｋｅｙ）は、「１０１０１１１０」であるものとする。

【０１９０】

暗号化装置、復号化装置がない場合、信号線のデータは、「００００１０１０１」より「１０１１０１１１」と変化する。従って、この場合、ビット反転数３に対応して、消費電力は３Ｐである。

【０１９１】

しかし、本例の場合、暗号化装置、即ち排他的論理和演算装置０６０３の働きにより、信号線０６０５に乗るデータは、鍵（Ｋｅｙ）「１０１０１１１０」と情報処理装置Ａ（ＣＰＵ）０６０１からのデータ「１０１１０１１１」とのビット毎の排他的論理和となる。即ち、その結果は「００００１１００１」である。

【０１９２】

このとき、信号線０６０５のデータは、信号線０６０５に直前に乗っていたデータ「００００１０１０１」より前述の排他的論理和の出力「００００１１００１」に変化することとなる。従って、この場合は、ビット反転数２に対応して、電力消費は２Ｐとなる。この電力消費は、暗号化装置、復号化装置がなく、本来消費されるはずの３Ｐとは異なる値である。

【０１９３】

データ処理装置Ｂ（ＲＡＭ）０６０２には、暗号化された値「０００１１００

１」 が格納される。この暗号化された値を再び信号線０６０５を通してデータ処理装置Ａ（ＣＰＵ）０６０１に返す時を考察してみる。

【０１９４】

データ処理装置Ｂ（ＲＡＭ）０６０２より信号線０６０５に出力されるデータは、「０００１１００１」より「０００１１００１」となって変化しない。従って、信号線０６０５は充放電せず、電力消費は行われない。

【０１９５】

この信号線０６０５よりの値は、復号化装置、即ち、排他的論理和演算装置０６０４の働きにより、信号線０６０５よりのデータ「０００１１００１」と鍵「１０１０１１１０」との排他的論理和「１０１１０１１１」がデータ処理装置Ａ（ＣＰＵ）０６０１に入力される。同一の数の排他的論理和は、０になるので、データ処理装置Ａ（ＣＰＵ）は矛盾なく演算が可能である。しかも信号線０６０５での充放電による消費電力は、本来のデータとは異なる。従って、消費電力を基礎として、元のデータを推測することが困難となる。

図１５は発明の第８の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る例であるが、更に、暗号化あるいは復号化する際、鍵（Ｋｅｙ）として乱数を用いる例である。本例では、データ処理装置より伝達するデータと乱数を用いて暗号化をはかり、一方、データ処理装置に伝達されるデータと前記と同様の乱数を用いて復号化を図るのである。

【０１９６】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）０７０１とデータ処理装置Ｂ（ＲＡＭ）０７０２とが信号線（バスライン）０７０５でつながれている。データ処理装置Ａ（ＣＰＵ）０７０１と信号線０７０５の間に暗号化装置および復号化装置を有する。暗号化装置としては排他的論理和演算装置０７０３及び、復号化装置としては排他的論理和演算装置０７０４が用いられる。

【０１９７】

そして、これらの暗号化装置および復号化装置に対する鍵として、乱数を用いる例である。従って、本例は乱数発生装置（ＲＮＧ）０７０６、および暗号化装

置０７０３および復号化装置０７０８への鍵バッファ０７０７、０７０８が準備されている。乱数発生装置自体等は通例のものを用いて十分である。

【０１９８】

乱数発生装置０７０６は、情報処理装置起動時のリセット信号（Ｒｅｓｅｔ）を受けて稼動し、８ビットの乱数を生成して停止し、再びリセット信号が入力されるまで停止したままである。また、鍵バッファ０７０７、０７０８は、前述の８ビットの乱数を格納するもので、８つのフリップフロップを有して構成されている。

【０１９９】

ここでは説明のため、信号線０７０５のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、信号線０７０５の制御方式はスタティック信号線制御方式であるものとする。尚、本実施の形態の効果はプリチャージ信号線制御方式においても同じである。

【０２００】

暗号化装置０７０３は、固定された８ビットの鍵（Ｋｅｙ）とデータ処理装置Ａ（ＣＰＵ）０７０１からの８ビットのデータとのビット毎の排他的論理演算を行なう装置である。又、復号化装置０７０４も同じ鍵とデータとのビット毎の排他的論理和演算を行なう装置である。

【０２０１】

リセット時に乱数生成装置０７０６を起動させて新たな８ビット鍵を設定する部分を除いて本実施例は、本発明の第６の実施の形態の実施例と同じで良い。従って、鍵バッファに乱数の鍵が設定されて以後の動作も第６の実施の形態の実施例と基本的に同様である。従って信号線での充放電による消費電力は本来のデータとは異なるものであり、さらに、暗号化に用いている鍵がリセット毎に変化するので、消費電力から元のデータを推測することがより困難となる。

【０２０２】

図１６は発明の第９の実施の形態を説明する為の情報処理装置の基本構成図で

ある。本例は信号線に乗せるデータの暗号化を図る別な例であり、更に暗号化装置が暗号鍵自動設定装置を有する例である。本例は特に暗号化の鍵情報の提供源に特徴がある。

【０２０３】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）０８０１とデータ処理装置Ｂ（ＲＡＭ）０８０２とがデータ信号線０８０６によってつながれている。暗号化装置としての排他的論理和演算装置０８０３、復号化装置としての排他的論理和演算装置０８０４、そして、鍵バッファ０８０５が設けられている。更に、データ処理装置Ａ（ＣＰＵ）０８０１とデータ処理装置Ｂ（ＲＡＭ）０８０２とに対してアドレス信号線上位４ビット０８０７、アドレス信号線下位４ビット０８０８が設けられる。

【０２０４】

ここでは説明のため、データ信号線０８０６のサイズは８ビットとし、アドレス信号線０８０７、０８０８のサイズも同じ８ビットであり、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、データ信号線０８０６及びアドレス信号線０８０７、０８０８の制御方式はスタティック信号線制御方式であるものとする。プリチャージ信号線制御方式においても本例の効果は同じである。

【０２０５】

暗号化装置０８０３は、固定された８ビットの鍵（Ｋｅｙ）とデータ処理装置Ａ（ＣＰＵ）０８０１からの８ビットのデータとのビット毎の排他的論理演算を行なう装置である。復号化装置も同じ鍵とデータとのビット毎の排他的論理和演算を行なう装置である。鍵バッファ０８０５の上位４ビットは固定された鍵であり、下位４ビットは、アドレス信号線の下位４ビットが格納されるものとする。図１６の鍵バッファ０８０５にこの旨を図示している。以下、鍵の固定部分の４ビットは、Ｄ（１６進数表現）であるものとする。

【０２０６】

データ処理装置Ａ（ＣＰＵ）０８０１がデータ処理装置Ｂ（ＲＡＭ）０８０２

のあるアドレスにデータを転送する場合を考える。今、データ処理装置Ｂ（ＲＡＭ）０８０２は、アドレスＦ０からアドレスＦＦまでとする。尚、ここで、この値は本質的ではない。

【０２０７】

データ処理装置Ａ（ＣＰＵ）０８０１は、表４に示す以下のデータを、アドレスＦ４から順に転送する。

【０２０８】

【表４】

Ａｄｄｒｅｓｓ	ＣＰＵからのデータ
F4	5D
F5	A0
F6	FE

表４

【０２０９】

データ処理装置Ａ（ＣＰＵ）０８０１からデータ５Ｄが転送される直前にデータ信号線０８０６に乗っていたデータは、ＣＦであるとする。データ５Ｄの転送が行われると、アドレス信号線には、Ｆ４が乗り、データ処理装置Ｂ（ＲＡＭ）０８０２の転送位置が確定する。

【０２１０】

データ５Ｄは、排他的論理和演算装置０８０３に入り、固定鍵４ビット Ｄ（１６進数表現）と、アドレスＦ４の下位４ビットの４との排他的論理和５Ｄｅｘｏｒ Ｄ４ ＝ ０１０１１１０１ ｅｘｏｒ １１０１０１００（２進数表現）＝ １０００１００１（２進数表現）＝ ８９（１６進数表現）が送信される。即ち、［固定鍵４ビット／アドレス下位４ビット］と［データ上位４ビット／データ下位４ビット］のビット毎の排他的論理和演算を行うことによって暗号化が行われた上で送信される。

【０２１１】

この８９（尚、この値は１６進数表現である。）が、データ信号線０８０６に乗ったときに消費される電力は、３Ｐとなる。それは、データが、ＣＦ（１１００１１１１）より８９（１０００１００１）と変化するので、ビット反転値が３であることによる。尚、ここで用いているＰは、本発明の第７の実施の形態において用いた記号である。即ち、Ｐは１ビットに対する消費電力である。

【０２１２】

以下同様のプロセスを経て、信号線０８０６に乗るデータは、ＣＦ（１１００１１１１）より８９（１０００１００１）へ、更にこの情報は７５（０１１１０１０１）、更に２８（００１０１０００）へと変化する。

【０２１３】

この変化に対応する信号線０８０５における消費電力は、３Ｐより６Ｐへ、更に２Ｐと変化する。

【０２１４】

これは本来の変化、ＣＦ（１１００１１１１）より５Ｄ（０１０１１１０１）、更にＡ０（１０１００００）よりＦＥ（１１１１１１１０）への変化とは異なっている。、即ち消費電力の変化として見れば、３Ｐより７Ｐへ、更に５Ｐへの変化に対応する。従って、半導体装置の消費電力の測定から、内部のデータを推測することが困難となる。

【０２１５】

図１７は発明の第１０の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例であるが、更に暗号化あるいは復号化装置がその設定手段を有する例である。

【０２１６】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）０９０１とデータ処理装置Ｂ（ＲＡＭ）０９０２とが信号線０９０７によってつながれている。本例は、暗号化装置としての排他的論理和演算装置０９０３、復号化装置としての排他的論理和演算装置０９０４を有し、且つ８ビットの鍵データを保持する鍵バッファ０９０５を有する。ここでは説明のため、信号線０９０７のサイズは８ビッ

トとし、データ処理装置Ａ（ＣＰＵ）０９０１は８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０２１７】

また、鍵バッファ０９０５は、データ処理装置Ａ（ＣＰＵ）０９０１に接続されている。そして、この鍵バッファ０９０５に、データ処理装置Ａ（ＣＰＵ）０９０１から書き込みを行うことができ、且つこの鍵バッファ０９０５はデータ処理装置Ｂ（ＲＡＭ）０９０２からの出力データの暗号化、入力データの復号化に用いられる。　データ処理装置Ａ（ＣＰＵ）０９０１から鍵の書き換えを行うことができることを除いて、その他の構成は本発明の第６の実施の形態における実施例と同様である。従って、その詳細説明は省略する。

【０２１８】

ここで前述の鍵バッファ０９０５の具体的な例を図４０に例示する。尚、ここに例示した鍵バッファは、例えば、以下に本願発明の実施の形態として例示する図２５、図２８および図２９などの鍵バッファ、１６０７、１４０６、１４０７、１６０７の実装例として適宜用い得ることは言うまでもない。

【０２１９】

図４０を用いて上述の鍵バッファを説明する。本例は、１ビットのシフトレジスタ１４６１、１４６２、１４６３、１４６４、１４６５、１４６６、１４６７、および１４６８、１ビットの排他的論理和演算装置１４７０、１４７１、１４７２、および乱数発生装置（ＲＮＧ）１４６９からなる。

【０２２０】

シフトレジスタ１４６１、１４６２、１４６３、１４６４、１４６５，１４６６、１４６７、および１４６８には、初期ビットが格納されているものとする。ここでは、説明のため、順に並べたとき１０１０１１１０となるものとしておく。一回のビットシフトを行う度に乱数発生装置１４６９は１ビットの欄数を発生するものとする。乱数は１ビットづつ発生し、例えば、０１１となったとする。この時、この鍵バッファが発生する８ビット値の列は、以下のようになる。

【０２２１】

１０１０１１１０－－＞０１０１１１００－－＞１０１１１１０１－－＞０１１１１１１１

この８ビットの振る舞いは、非常に乱数に近いことが知られている。一般に、正しい乱数の発生には時間がかかることが多い。しかし、本例のそれは、１ビットの乱数を用いるだけで、８ビットの（疑似）乱数列を生成することができる。従って、本例の乱数発生の手段によって、極めて高速な処理が可能となる。このように高速動作の疑似乱数発生手段によって、極めて実用的な情報処理装置を提供することが出来る。

【０２２２】

図１８は発明の第１１の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。更に、本例は鍵選択装置（マルチプレクサ）を用いて鍵（Ｋｅｙ）を選択する例である。

【０２２３】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１００１とデータ処理装置Ｂ（ＲＡＭ）１００２とがデータ信号線１００９でつながれている。暗号化装置として排他的論理和演算装置１００３、復号化装置として排他的論理和演算装置１００４が用いられる。

【０２２４】

鍵選択装置（マルチプレクサ）１００６、１０１４、鍵テーブル１００７、１０１５、鍵バッファ１００８、１０１３、鍵番号転送用信号線１０１０を有する。尚、前記鍵テーブル１００７、１０１５は固定されたもので、書き換えできないものとする。そして、鍵テーブル１００７、１０１５にはＫｅｙ０とＫｅｙ１が格納されている。勿論、本願発明において、鍵テーブルとして書き換え可能な鍵テーブルを用いることも可能である。鍵選択装置１００６は鍵バッファ１００８に接続され、暗号化装置１００３に対して用いられる。鍵選択装置１０１４は鍵バッファ１０１３に接続され、復号化装置１００４に対して用いられる。鍵番号転送用信号線１０１０によって鍵番号が転送される。

【０２２５】

ここでは説明を容易にするのため、信号線１００９のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０２２６】

本例によれば、ユーザ（例えばＩＣカードのアプリケーションを制作する企業）は、鍵テーブル１００７のどの鍵を用いて暗号化するのかを、鍵選択ビットバッファ１０１１に指定することで選択できる。以下、鍵選択ビットバッファ１０１１に格納された値をＳＫＥＹＢＩＴと呼ぶ。

【０２２７】

鍵選択装置１００６は、鍵選択ビットバッファ１０１１に格納されたＳＫＥＹＢＩＴを参照して、鍵テーブル１００７中から用いるべきＫｅｙを取り出し、鍵バッファ１００８に格納する。ここで、ＳＫＥＹＢＩＴが０であれば、鍵選択装置（マルチプレクサ）１００６は、鍵テーブル１００７のＫｅｙ０を選択し、鍵バッファ１００８に格納し、もしＳＫＥＹＢＩＴが１であれば、鍵テーブル１００７のＫｅｙ１を選択し、鍵バッファ１００８に格納する。

【０２２８】

データ処理装置Ａ（ＣＰＵ）１００１が、データ処理装置Ｂ（ＲＡＭ）１００２にデータを転送する際、排他的論理和演算装置１００３によって鍵バッファ１０１１に格納されている８ビットの鍵データとデータ処理装置Ａ（ＣＰＵ）１００１からの８ビットのデータとの排他的論理和がとられる。そして、この値がデータ信号線１０１０に乗せられて、データ処理装置Ｂ（ＲＡＭ）１００２に転送される。同時に、鍵選択ビットバッファ１０１１に格納されているＳＫＥＹＢＩＴの値を鍵番号転送用信号線１０１０を通してデータ処理装置Ｂ（ＲＡＭ）１００２に転送される。このとき、データ処理装置Ｂ（ＲＡＭ）１００２内のデータは、表５に示される形で格納される。

【０２２９】

【表５】

ＳＫＥＹＢＩＴ（１ｂｉｔ）	ＤＡＴＡ（８ｂｉｔ）

表５

【０２３０】

これは、ＤＡＴＡが、鍵番号がＳＫＥＹＢＩＴとなる鍵によって暗号化されていることを示している。鍵選択ビットバッファ１０１１内のＳＫＥＹＢＩＴがプログラム等によって書き換えられた場合は、別の鍵によって暗号化される。例えば、データ処理装置Ｂ（ＲＡＭ）の内部データは、次のようなものになる。

【０２３１】

１　ＥＦ

０　Ａ３

１　３Ｅ

１　５４

０　３Ｄ

これらのデータを、再びデータ処理装置Ａ（ＣＰＵ）１００１に戻して用いるときには、次の動作を行なう。これら暗号化データを転送する前に、データ処理装置Ｂ（ＲＡＭ）１００２より、鍵番号転送用信号線１０１０を通して鍵選択ビットを鍵選択装置１０１４に転送する。鍵選択装置１０１４は、鍵選択ビットに応じて鍵テーブル１０１５に格納された鍵を選択し、鍵バッファ１０１３に転送する。その上でデータ処理装置Ａ（ＣＰＵ）１００１は、データ処理装置Ｂ（ＲＡＭ）１００２に対してデータを要求し、データ処理装置Ｂ（ＲＡＭ）１００２の該当データをデータ信号線１００９に乗せる。更に、排他的論理和演算装置１００４によって該当データと鍵バッファ１０１３に格納された鍵との排他的論理和をとり、データ処理装置Ａ（ＣＰＵ）１００１に入力する。データの暗号化に

用いた鍵番号に応じて復号化が行われるので、データ処理装置Ａ（ＣＰＵ）１００１では矛盾なく処理が行われる。

【０２３２】

図１９は発明の第１２の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は、信号線のデータを暗号化して伝達するひとつの例である。更には、本例は記憶装置を複数の領域に分割し、領域毎に暗号化するか否かを指定して、暗号化、復号化する方法である。

【０２３３】

本実施例の情報処理装置は、データ処理装置５１１０１と情報記憶装置５１１０２とがデータバス５１１０７によってつながれている。データ処理装置５１１０１に暗号化装置５１１０３および複号化装置５１１０４が設けられている。そして、本例では、暗号化判定回路７３１２によって暗号するか否かを判定して、この情報を暗号化装置５１１０３および複号化装置５１１０４に与えられる。この動作の為、暗号鍵記憶装置５１１０６、暗号化領域指定レジスタ７３１１、暗号化判定回路７３１２、ＡＮＤ回路５１１１２などが設けられている。更に、本例は情報記憶装置とデータ処理装置の間にはアドレスバス５１１０８を有する。

【０２３４】

ここで、情報記憶装置５１１０２自体の構成は、通例に従って十分である。情報記憶装置の記憶領域は、記憶領域のアドレス値によって複数の領域に分類され、それぞれの領域に対して暗号化を行うか否かを、暗号化領域指定レジスタ７３１１で指定する。暗号化判定回路７３１２は、アドレスバス５１１０８に現れるアドレス値と、暗号化領域指定レジスタ７３１１の値によって、暗号化を行うか判定する。

【０２３５】

図２０は、暗号化判定回路のひとつの実施例を示す。この暗号化判定回路の例では、メモリを分割する際の上位ｐビット分を参照し、メモリアレイの領域をｐビットのそれぞれの状態で識別し、２＾ｐの領域に分割する。暗号化領域指定レジスタ７３１１は、２＾ｐビットの長さを持ち、各ビットはメモリアレイ上の１つの領域と対応し、暗号化を行うか否かを制御する。

【０２３６】

暗号化領域指定レジスタ７３１１の各ビットと、該ビットに相当するアドレス領域を表すビットパタンに対して、ビットがすべて１となるようにＮＯＴを挟んだのち、暗号化領域指定レジスタの該当ビットとの論理積をとる。この論理積が１のときは、暗号化を行い、０の時は暗号化を行わない。暗号化領域指定レジスタ７３１１の各ビットに対して同様の回路を作り、その後論理積すべてのビットの論理和を論理和演算装置７３１４で取る。この論理和が１のときは、暗号化を行い、０の時は暗号化を行わないようにする。

【０２３７】

暗号化判定回路７３１２の出力は、暗号鍵とのＡＮＤが論理積演算装置５１１１２で計算され、暗号化装置５１１０３複号化装置５１１０４にそれぞれ送られる。論理積演算装置５１１１２の出力は、暗号化を行う際には、暗号鍵と同じ値になるが、暗号化を行わないときには、０となる。暗号化装置５１１０３は、暗号鍵として０が与えられると、入力と出力が等しくなるので、暗号化を行わないのと等価になる。

【０２３８】

読み出し時の複号化の手順は、書き込みと同様、アドレスの値と暗号化領域指定レジスタ７３１１の値によって、複号化を行う際の暗号鍵を０とするか暗号鍵の値にするかを制御し、複号化を行う。

【０２３９】

このようにして、情報記憶装置をアドレスによって複数領域に分割して、それぞれの領域ごとに暗号化の有無が設定できる。暗号化を施された領域では、データバス５１１０７に現れるビットパタンや情報記憶装置に記録されるデータのビットパタンは実際のデータとは異なるため、情報記憶装置へのデータの書き込み・読み込み時の消費電流パタンやバスで消費される電流パタンから実際のデータを推測する事が困難となる。

【０２４０】

図２１は発明の第１３の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化複号化を図る別な

例である。本例は特定のデータパターンに対しては暗号化を行わない例である。

【０２４１】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１１０１とデータ処理装置Ｂ（ＲＡＭ）１１０２とが信号線１１０９でつながれている。暗号化装置としては排他的論理和演算装置１１０３、復号化装置としては排他的論理和演算装置１１０４が設けられている。この暗号化装置および復号化装置に対する鍵選択の為にラッチ回路１１０５、８ビットの暗号化禁止データバッファ１１０６、復号化禁止データバッファ１１１３、鍵テーブル１１０７、１１１２、鍵選択装置１１０８、１１１１、など設けられている。

【０２４２】

ここで、復号化禁止データバッファ１１１３の内部のデータは、暗号化禁止データバッファ１１０６内部のデータと同じデータが格納されている。また、鍵テーブル１１０７と１１１２とは全く同じ鍵データが格納されている。

【０２４３】

ここでは説明のため、信号線０７０５のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０２４４】

鍵テーブル１１０７には、暗号化用の鍵（Ｋｅｙ）及び、０が格納されているものとする。暗号化禁止データバッファ１１０６及び、復号化禁止データバッファ１１１３には、禁止データ（ＦＤＡＴＡ）及び、ＦＤＡＴＡと暗号化鍵（Ｋｅｙ）との排他的論理和の値が格納されている。このＦＤＡＴＡとＫｅｙの排他的論理和の値をＣＯ－ＦＤＡＴＡと呼ぶ。ＣＯ－ＦＤＡＴＡが必要な理由は、次のようである。データとＫｅｙとの排他的論理和がＦＤＡＴＡに一致してしまった場合、この暗号化データをデータ処理装置Ｂ（ＲＡＭ）１１０２からデータ処理装置Ａ（ＣＰＵ）１１０１に戻したときに、暗号化がなされたままデータ処理装置Ａ（ＣＰＵ）１１０１に入力され、処理が矛盾するからである。

【０２４５】

鍵（Ｋｅｙ）との排他的論理和がＦＤＡＴＡに一致するのは、ＣＯ－ＦＤＡＴＡだけであるから、暗号化禁止データバッファ１１０６及び復号化禁止データバッファ１１１３に格納しなければならないデータは、禁止データ（ＦＤＡＴＡ）及びＣＯ－ＦＤＡＴＡだけである。

【０２４６】

データ処理装置Ａ（ＣＰＵ）１１０１からデータ処理装置Ｂ（ＲＡＭ）１１０２に信号線１１０９を通してデータを転送する際、該データは、鍵選択装置１１０８及び、ラッチ回路１１０５に入力される。ラッチ回路１１０５は、鍵選択装置１１０８からデータ保持解除信号の値（ＯＵＴＤＡＴＡ－ＢＩＴ）が１になるまで、該データを保持し続け、ＯＵＴＤＡＴＡ－ＢＩＴが１になると、保持を解除し、排他的論理和演算装置１１０３に入力される。鍵選択装置１１０８に入力されたデータは、暗号化禁止データバッファ１１０６に保持されている８ビットの暗号化禁止データ（ＦＤＡＴＡ）及びＣＯ－ＦＤＡＴＡと比較される。そして、鍵選択装置１１０８に入力されたデータがそのいずれか一方と同じであれば、鍵テーブル１１０７より値０を選択して保持し、ラッチ回路１１０５にＯＵＴＢＩＴ－ＤＡＴＡ１を送るとともに、排他的論理和演算装置１１０３に値０を送信する。任意のビット値ｘと０との排他的論理和がｘに等しいので、このときには該データは暗号化されずに信号線１１０９に乗せられ、データ処理装置Ｂ（ＲＡＭ）に入力される。

【０２４７】

一方、ＦＤＡＴＡまたはＣＯ－ＦＤＡＴＡと該データが同一でない場合は、鍵テーブルより値Ｋｅｙを選択して保持し、ラッチ回路１１０５にＯＵＴＢＩＴ－ＤＡＴＡ１を送るとともに、排他的論理和演算装置１１０３に値Ｋｅｙを送信する。このとき、該データは暗号化されて信号線１１０９に乗せられ、データ処理装置Ｂ（ＲＡＭ）に入力される。逆に情報処理装置Ｂ（ＲＡＭ）のデータをデータ処理装置Ａ（ＣＰＵ）に転送するときには、そのまま信号線１１０９に乗せて転送を行う。このときも、以上と同様のプロセスでデータとＦＤＡＴＡまたはＣＯ－ＦＤＡＴＡが一致したときには復号化されず、不一致のときには同じＫｅｙ

による復号化がなされ、矛盾なく処理が行われる。

【０２４８】

図２２は発明の第１４の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータを暗号化する別な例である。更には本例はデータを伝達する両データ処理装置と信号線の間の双方に暗号化および復号化装置を挿入する例である。

【０２４９】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１３０１とデータ処理装置Ｂ（ＲＡＭ）１３０２とが信号線１３０７でつながれている。暗号化装置としては排他的論理和演算装置１３０３、１３０５、復号化装置としては排他的論理和演算装置１３０４、１３０６が用いられる。排他的論理和演算装置１３０３、１３０４、１３０５、１３０６は、全て同一の鍵 Ｋｅｙ とデータとの排他的論理和を計算して出力するものである。データ処理装置Ａ（ＣＰＵ）１３０１から出力されたデータは、排他的論理和演算装置１３０３によって暗号化され、信号線１３０７を通してデータ処理装置Ｂ（ＲＡＭ）１３０２に転送される。しかし、一方、データ処理装置Ｂ（ＲＡＭ）１３０２に入力される前に排他的論理和演算装置１３０６によって復号された後、データ処理装置Ｂ（ＲＡＭ）１３０２に入力される。

【０２５０】

本発明の第６の実施の形態とは異なり、本実施例においては、データ処理装置Ｂ（ＲＡＭ）１３０２内のデータは、暗号化されていない元のデータとなる。また、データ処理装置Ｂ（ＲＡＭ）１３０２内のデータがデータ処理装置Ａ（ＣＰＵ）１３０１に転送されるときには、排他的論理和演算装置１３０５によって暗号化が行われ、信号線１３０７を通してデータ処理装置Ａ（ＣＰＵ）１３０１に転送されるが、データ処理装置Ａ（ＣＰＵ）１３０１に入力される前に排他的論理和演算装置１３０４によって復号された後、データ処理装置Ａ（ＣＰＵ）１３０１に入力される。

【０２５１】

このとき、信号線における充放電は、本発明の第６の実施の形態における情報

処理装置におけるものと全く同じである。

【０２５２】

図２３は発明の第１５の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。本例はデータ処理装置と信号線の間に暗号化および復号化装置ならびに鍵情報を設定する装置を挿入する例である。

【０２５３】

本実施例の情報処理装置は、本発明の第６の実施の形態の情報処理装置の実施例を双方向化したものである。本例は、データ処理装置Ａ（ＣＰＵ）１４０１、データ処理装置Ｂ（ＲＡＭ）１４０２、信号線１４１０、暗号化装置としての排他的論理和演算装置１４０３、１４１１及び、復号化装置としての排他的論理和演算装置１４０４、１４１２、乱数発生装置（ＲＮＧ）１４０９、鍵バッファ１４０５、１４０６、１４０７、１４０８を有する。

【０２５４】

乱数発生装置１４０９は、情報処理装置起動時のリセット信号（Ｒｅｓｅｔ）を受けて稼動し、８ビットの乱数を生成して停止し、再びリセット信号が入力されるまで停止したままである。また、鍵バッファは、８ビットの乱数を格納するもので、８つのフリップフロップから構成される。ここでは説明のため、信号線１４１０のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、信号線１４１０の制御方式はスタティック信号線制御方式であるものとする。尚、プリチャージ信号線制御方式においても本例の効果は同じである。

【０２５５】

リセット時に乱数生成装置１４０９を起動させて新たな８ビット鍵を設定する部分を除いて本実施例は、本発明の第１３の実施の形態における情報処理装置と同じものである。従って、鍵バッファに乱数の鍵が設定されて以後の動作も同様である。動作の詳細説明は省略する。

【０２５６】

本例においても、当然、信号線での充放電による消費電力は本来のデータとは異なるものであり、さらに、暗号化に用いている鍵がリセット毎に変化するので、消費電力から元のデータを推測することが困難となる。

【０２５７】

図２４は発明の第１６の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。本例は暗号化に用いる鍵情報の一部として記憶装置の番地情報を用いる例である。

【０２５８】

本実施例の情報処理装置は、基本的に本発明の第７の実施の形態の情報処理装置を双方向化したものである。本例は、データ処理装置Ａ（ＣＰＵ）１５０１、データ処理装置Ｂ（ＲＡＭ）１５０２、暗号化装置としての排他的論理和演算装置１５０３、１５０５、復号化装置としての排他的論理和演算装置１５０４、１５０６、鍵バッファ１５０７、データ信号線１５１０、アドレス信号線上位４ビット１５０８、アドレス信号線下位４ビット１５０９を有する。ここでは説明のため、データ信号線１５１０のサイズは８ビットとし、アドレス信号線１５０８、１５０９のサイズも同じ８ビットであり、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。また、データ信号線１５１０及びアドレス信号線１５０８、１５０９の制御方式はスタティック信号線制御方式であるものとする。プリチャージ信号線制御方式においても本例の効果は同じである。

【０２５９】

暗号化装置は、固定された８ビットの鍵（Ｋｅｙ）とＣＰＵからの８ビットのデータとのビット毎の排他的論理演算装置であり、復号化装置も同じ鍵とデータとのビット毎の排他的論理和演算装置である。鍵バッファ１５０７の上位４ビットは固定された鍵であり、下位４ビットは、アドレス信号線下位４ビット１５０９のデータが格納されるものとする。

【０２６０】

データ処理装置Ａ（ＣＰＵ）からデータが転送される場合の動作は、本発明の第７の実施の形態の情報処理装置において説明したものと同じである。

【０２６１】

しかし、データ信号線１５１０に暗号化されたまま入力されるのではなく、鍵バッファ１５０７に格納されている暗号化鍵を用いて復号化されてからデータ処理装置Ｂ（ＲＡＭ）１５０２に入力される。逆に、データ処理装置Ｂ（ＲＡＭ）１５０２の内部のデータをデータ処理装置Ａ（ＣＰＵ）１５０１に転送するときには、データ処理装置Ａ（ＣＰＵ）１５０１から、対応するアドレスがアドレス線１５０８、１５０９によって転送され、その値を用いて鍵バッファ１５０７の値が決定される。そして、この鍵バッファ１５０７の値とデータとの排他的論理和が、データ信号線１５１０に乗せられる。排他的論理和演算装置１５０４によって、この値と暗号化に用いた鍵バッファ１５０７の鍵との排他的論理和をとることによって復号し、データ処理装置Ａ（ＣＰＵ）に入力される。このとき、信号線における充放電の動作は、前述の第７の実施の形態の情報処理装置の実施例におけるものと全く同じである。

【０２６２】

図２５は発明の第１７の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。更には本例はデータ処理装置と信号線の間に暗号化および復号化装置を挿入し、且つ暗号化に用いる鍵情報を自動的に再設定する例である。

【０２６３】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１６０１、データ処理装置Ｂ（ＲＡＭ）１６０２、暗号化装置としての排他的論理和演算装置１６０３、１６０５、復号化装置としての排他的論理和演算装置１６０４、１６０６、８ビットの鍵を格納する鍵バッファ１６０７、乱数生成装置（RNG）１６０８、５ビット入力１出力の論理和演算装置１６０９、５ビットの大きさを持つカウンタ１６１０、信号線１６１１から構成される。カウンタ１６１０は、クロック信号（ＣＬＫ）のエッジの立ち上がりに合わせてカウントを行い、５ビットより大

きな部分は無視される。ここでは説明のため、信号線１６１１のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０２６４】

データ処理装置Ａ（ＣＰＵ）１６０１からデータ処理装置Ｂ（ＲＡＭ）１６０２にデータを転送する場合、データ処理装置Ａ（ＣＰＵ）１６０１は、クロック信号に同期してデータを転送する。クロック信号が発信されると、カウンタ１６１０はカウントを始める。論理和演算装置１６０９は、カウンタの各ビット全てに対する論理和を乱数生成装置１６０８に送信する。乱数生成装置１６０８は、該論理和の値が０であれば、８ビットの乱数を生成し、該８ビット乱数を鍵バッファ１６０７に送信して停止する。このとき、カウンタの値が全て０になったときのみ、乱数生成装置１６０８は、０を受け取るので、鍵は３２クロック毎に暗号化、復号化に用いる鍵を交換することになる。鍵バッファ１６０７は、排他的論理和演算装置１６０３、１６０４、１６０５、１６０６全てに同一の鍵を供給する。

【０２６５】

データ処理装置Ａ（ＣＰＵ）からデータをデータ処理装置Ｂ（ＲＡＭ）に信号線１６１１を通して転送する際、まず、排他的論理和演算装置１６０３にて鍵バッファ１６０７の値とデータとの排他的論理和を信号線１６１１に乗せて転送する。この暗号化されたデータは、データ処理装置Ｂ（ＲＡＭ）に入る前に同じ鍵バッファ１６０７の値との排他的論理和が取られるので、復号されて元のデータ値になり、データ処理装置Ｂ（ＲＡＭ）１６０２に入力される。データ処理装置Ｂ（ＲＡＭ）１６０２のデータをデータ処理装置Ａ（ＣＰＵ）１６０１に転送する場合も同様である。

【０２６６】

図２６は発明の第１８の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータの暗号化を図る別な例である。本例はデータ処理装置Ａ（ＣＰＵ）１７０１から鍵の書き換えを行うことが

できる例である。

【０２６７】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１７０１、データ処理装置Ｂ（ＲＡＭ）１７０２、暗号化装置としての排他的論理和演算装置１７０３、１７０５、復号化装置としての排他的論理和演算装置１７０４、１７０６、８ビットを格納する鍵バッファ１７０７、信号線１７０９から構成される。ここでは説明のため、信号線１７０９のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０２６８】

鍵バッファ１７０７はＣＰＵ１７０１に接続されており、ＣＰＵ１７０１から鍵バッファ１７０７の内容を変更することが可能である。鍵バッファ１７０７に保持された鍵情報は、データ処理装置Ａ（ＣＰＵ）１７０１からの出力データの暗号化、入力データの復号化に用いられる。データ処理装置Ａ（ＣＰＵ）１７０１から鍵の書き換えを行うことができることを除いて、その他の構成は本発明の第１５の実施の形態における実施例と同様である。

【０２６９】

図２７は発明の第１９の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は信号線に乗せるデータを暗号化し、且つ復号化してデータを格納する例である。

【０２７０】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１３０１、データ処理装置Ｂ（ＲＡＭ）１３０２、暗号化装置としての排他的論理和演算装置１３０３、復号化装置としての排他的論理和演算装置１３０６、信号線１３０７から構成されている。排他的論理和演算装置１３０３、１３０６は、全て同一の鍵Ｋｅｙとデータとの排他的論理和を計算して出力するものである。

【０２７１】

データ処理装置Ａ（ＣＰＵ）１３０１から出力されたデータは、排他的論理和

演算装置１３０３によって暗号化され、信号線１３０７を通してデータ処理装置Ｂ（ＲＡＭ）１３０２に転送されるが、データ処理装置Ｂ（ＲＡＭ）１３０２に入力される前に排他的論理和演算装置１３０６によって復号された後、データ処理装置Ｂ（ＲＡＭ）１３０２に入力される。

【０２７２】

本発明の第６の実施の形態とは異なり、本実施例においては、データ処理装置Ｂ（ＲＡＭ）１３０２内のデータは、暗号化されていない元のデータとなる。このとき、データ処理装置Ａ（ＣＰＵ）１３０１から、データ処理装置Ｂ（ＲＡＭ）１３０２に送られる情報は、信号線上では暗号化されている。従って、信号線の充放電電流からは、送られた情報を推測することは困難になる。

【０２７３】

図２８は発明の第２０の実施の形態を説明する為の情報処理装置の概要を説明する基本構成図である。本例は本例は信号線に乗せるデータを暗号化し、且つ復号化してデータを格納する例である。更には、本例は乱数を用いた鍵をもちいた例である。

【０２７４】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１４０１、データ処理装置Ｂ（ＲＡＭ）１４０２、信号線１４１０、暗号化装置としての排他的論理和演算装置１４０３及び、復号化装置としての排他的論理和演算装置１４１２、乱数発生装置（ＲＮＧ）１４０９、鍵バッファ１４０６、１４０７から構成される。

【０２７５】

乱数発生装置１４０９は、情報処理装置起動時のリセット信号（Ｒｅｓｅｔ）を受けて稼動し、８ビットの乱数を生成して停止し、再びリセット信号が入力されるまで停止したままである。また、鍵バッファは、８ビットの乱数を格納するもので、８つのフリップフロップから構成される。ここでは説明のため、信号線１４１０のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである

。また、信号線１４１０の制御方式はスタティック信号線制御方式であるものとする。プリチャージ信号線制御方式においても本例の効果は同じである。

【０２７６】

リセット時に乱数生成装置１４０９を起動させて新たな８ビット鍵を設定する部分を除いて本実施例は、本発明の第１９の実施の形態における情報処理装置の実施例と同じものである。従って、鍵バッファに乱数の鍵が設定されて以後の動作も同様である。従って信号線での充放電による消費電力は本来のデータとは異なるものであり、さらに、暗号化に用いている鍵がリセット毎に変化するので、消費電力から元のデータを推測することが困難となる。

【０２７７】

図２９は発明の第２１の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る例である。更には、本例は乱数を用いて鍵情報を設定する例である。

【０２７８】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）１６０１、データ処理装置Ｂ（ＲＡＭ）１６０２、暗号化装置としての排他的論理和演算装置１６０３、復号化装置としての排他的論理和演算装置１６０６、８ビットの鍵を格納する鍵バッファ１６０７、乱数生成装置（ＲＮＧ）１６０８、５ビット入力１出力の論理和演算装置１６０９、５ビットの大きさを持つカウンタ１６１０、信号線１６１１から構成される。カウンタ１６１０は、クロック信号（ＣＬＫ）のエッジの立ち上がりに合わせてカウントを行い、５ビットより大きな部分は無視される。ここでは説明のため、信号線１６１１のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０２７９】

本例では、データ処理装置Ａ（ＣＰＵ）１６０１からデータ処理装置Ｂ（ＲＡＭ）１６０２にデータを転送する場合、データ処理装置Ａ（ＣＰＵ）１６０１は、クロック信号に同期してデータを転送する。クロック信号が発信されると、カ

ウンタ１６１０はカウントを始める。論理和演算装置１６０９は、カウンタの各ビット全てに対する論理和を乱数生成装置１６０８に送信する。乱数生成装置１６０８は、該論理和の値が０であれば、８ビットの乱数を生成し、該８ビット乱数を鍵バッファ１６０７に送信して停止する。このとき、カウンタの値が全て０になったときのみ、乱数生成装置１６０８は、０を受け取るので、鍵は３２クロック毎に暗号化、復号化に用いる鍵を交換することになる。鍵バッファ１６０７は、排他的論理和演算装置１６０３、　１６０６全てに同一の鍵を供給する。

【０２８０】

データ処理装置Ａ（ＣＰＵ）からデータをデータ処理装置Ｂ（ＲＡＭ）に信号線１６１１を通して転送する際、まず、排他的論理和演算装置１６０３にて鍵バッファ１６０７の値とデータとの排他的論理和を信号線１６１１に乗せて転送する。この暗号化されたデータは、データ処理装置Ｂ（ＲＡＭ）に入る前に同じ鍵バッファ１６０７の値との排他的論理和が取られるので、復号されて元のデータ値になり、データ処理装置Ｂ（ＲＡＭ）１６０２に入力される。信号線１６１１での充放電による消費電力は、本来のデータとは異なるものであり、さらに、暗号化に用いている鍵が定期的に変化する。従って、信号線１６１１での消費電力から元のデータを推測することが困難となる。

【０２８１】

図３０は発明の第２２の実施の形態を説明する為の情報処理装置の基本構成図である。本例は信号線に乗せるデータの暗号化を図る例である。更には、本例は鍵情報の設定、変更が出来る装置を有する例である。

【０２８２】

本実施例の情報処理装置は、データ処理装置Ａ（ＣＰＵ）、データ処理装置Ｂ（ＲＡＭ）、暗号化装置としての排他的論理和演算装置１７０３、復号化装置としての排他的論理和演算装置１７０６、８ビットを格納する鍵バッファ１７０７、信号線１７０９から構成される。ここでは説明のため、信号線１７０９のサイズは８ビットとし、ＣＰＵは８ビットプロセッサであるものとする。信号線のサイズ、ＣＰＵのビット数は、本発明において本質的ではない。従って、前述の条件の説明で、本願発明一般を説明して十分納得されるものである。

【０２８３】

鍵バッファ１７０７はデータ処理装置Ａ（ＣＰＵ）１７０１に接続されており、データ処理装置Ａ（ＣＰＵ）１７０１から鍵バッファ １７０７の内容を変更することが可能である。鍵バッファ１７０７に保持された鍵情報は、データ処理装置Ａ（ＣＰＵ）１７０１からデータ処理装置Ｂ（ＲＡＭ）へ信号線１７０９を通じて送られるデータの暗号化および複号化の双方に使われる。データ処理装置Ａ（ＣＰＵ）１７０１から鍵の書き換えを行うことができることを除いて、その他の構成は本発明の第１９の実施の形態と同様である。従って、その動作の詳細説明は省略する。

【０２８４】

尚、以下の第２３より第２９までの発明の実施の形態はいわゆる半導体記憶装置あるいはより大きい情報処理装置に含まれる半導体記憶装置の部分に本願発明の基本思想を適用した例である。従って、以下の第２３より第２９までの発明の実施の形態を、例えば、いわゆるマイクロコンピュータ・システムに含まれる記憶部に適用することが出来る。更には、こうした大きな半導体装置システムの記憶部に本例の如き方法を適用し、更に、全体システムの情報の処理に際して、上記した本願諸発明を合わせて適用することも当然可能である。

【０２８５】

図３１は発明の第２３の実施の形態を説明する為の情報処理装置の基本構成図である。

【０２８６】

第２３の実施例の情報記憶装置７００１は、いわゆる半導体記憶装置の例である。

【０２８７】

本半導体記憶装置は、基本的な半導体記憶装置と同様に、メモリセルアレイ７００２、アドレスデコーダ７００５、およびデータバス７００７を有して構成される。そして、本例は、信号の暗号化の為に、暗号化装置７００３、複号化装置７００４、暗号鍵記憶装置７００６を有する。

【０２８８】

ここで、メモリセルアレイ７００２の構成自体は、通例に従って十分である。メモリセルは多くの例は１トランジスタ、１キャパシタンスで構成される。更にまた、その他の形態もとることが出来る。

【０２８９】

図３２はメモリセルアレイ７００２の代表的な例を示す回路図である。図３２に点線で囲った領域６６が１つのメモリセルに当たる領域である。各メモリセル６６は各ビット線６５によってそれぞれセンスアンプ６０、６１に接続される。一方、各ワード線６４によってそれぞれワード線ドライバ６２、６３に接続されている。こうした半導体メモリ装置に対して本願発明に技術思想を適用して、セキュリティに関して極めて有用な効果を奏する。尚、図３２に示したセンスアンプ６０、６１の出力は、例えば図３１のメモリセルアレー７００２の読み出しデータとなる。一方、メモリセルアレイ７００２の書き込みデータに従い、ビット線６６を通して、ワード線により選択されたメモリセル６６のキャパシタンスを充放電する。尚、以下に示すメモリセルアレーを用いた本願発明の実施の諸形態に本例のメモリセルアレーを用いて十分である。勿論、本願発明の他の実施の形態として、メモリセルアレーを他の形態のものを用い得ることは言うまでもない。

【０２９０】

以下に本例の動作の詳細を説明する。メモリアレイ７００２へのデータの書き込みは、次のような動作である。データが、データバス７００７より暗号化装置７００３に送られる。そして、暗号化装置７００３では、暗号鍵記憶装置（鍵バッファ）７００６内の情報を参照して、暗号化装置７００３によって、データが暗号化される。一方、アドレスバス７００８で指定されたアドレスが、アドレスデコーダ７００５によりでコード化され、ワード選択信号としてメモリセルアレイ７００２に送られる。メモリセルアレーでは、このコード化されたアドレスによって、データを書き込むべきメモリセルが選択される。そして、メモリセルには、暗号化処理装置７００３により暗号化されたデータが書き込まれる。

【０２９１】

また、メモリセルアレイ７００２からのデータの読み出しは、、次のような動作である。アドレスバス７００８で指定されたアドレスが、アドレスデコーダ７００５によりデコードされ、ワード選択信号としてメモリセルアレイ７００２に送られる。そして、ワード選択信号によって選択されたメモリセルの内容が読み出される。読み出されたメモリセルの内容は、複号化装置７００４に送られる。複号化装置７００４は、暗号鍵格納装置（鍵バッファ）７００６より取り出した暗号鍵情報を参照して、複号化する。こうして、復号化されたデータはデータバス７００７に出力する。尚、ここで、暗号鍵記憶装置７００６の鍵情報は、その外部より書き換えることが出来る。本願明細書における本実施例以外の例における暗号鍵記憶装置に関しても同様のことが言える。

【０２９２】

このようにこの発明のひとつの実施例では、データバス７００７から送られてきたデータをメモリセルアレイ７００２に格納する前に暗号化が施され、メモリセルアレイ７００２からデータを読み出す際には複号化が施されてデータバス７００７に出力される。

【０２９３】

従って、メモリセルアレイを含む半導体装置においても、これまで説明してきた諸情報処理装置と同等に扱える。この結果、メモリセル上に実際に記録されるデータのビットパタンは、記憶させようとしたデータとは異なるため、セル上のデータの書き込み・読み込み時の消費電流パタンからセル上のデータを推測する事が困難になる。

【０２９４】

このように、通例のメモリセルを有する半導体記憶装置に対しても、本願の発明諸思想を適用することが出来る。本例ならびに以下の諸例に限らないことは言うまでもない。尚、上述の例では、一般的なマトリクス状のメモリアレの行の選択についてのアドレスを言及した。しかし、当該メモリアレーの列に対して本例の発明思想を適用することが出来る。更に、メモリアレーの行列の双方に本願の発明思想を適用することも出来る。

【０２９５】

これを背景として、以下の実施の諸形態において、いわゆる半導体記憶装置を情報処理装置と称する。従って、本願明細書において、情報処理装置はいわゆる半導体記憶装置をも含むものである。

【０２９６】

図３３は発明の第２４の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置の例である。本例は暗号化に当って、暗号化鍵を用いる。

【０２９７】

本実施例の情報記憶装置は、通例の半導体記憶装置と同様に、メモリセルアレイ７００２、アドレスデコーダ７００５およびデータバス７００７を有する。そして、本例は、信号の暗号化および復号化の為、暗号化装置７００３、複号化装置７００４、暗号鍵記憶装置７００６、暗号鍵記憶装置の鍵と、アドレス情報の一部から新たな暗号化鍵を生成するためのＥＯＲ回路７１０９を有する。ここで、メモリセルアレイ７００２の構成は、通例に従って十分である。

【０２９８】

メモリアレイ７００２へのデータの書き込みは、次のような動作である。

【０２９９】

データが、データバス７００７より暗号鍵記憶装置７００６に送られる。そして、暗号鍵記憶装置７００６では、暗号鍵記憶装置７００６内の情報とアドレスバス７００８の情報を排他的論理和演算装置７１０９で合成する。こうして得られる暗号鍵を用いて、データバス７００７から送られたデータは暗号化装置７００３によって暗号化される。一方、アドレスバス７００８で指定されたアドレスが、アドレスデコーダ７００５によりでコード化され、ワード選択信号としてメモリセルアレイ７００２に送られる。

【０３００】

メモリセルアレーでは、このコード化されたアドレスによって、データを書き込むべきメモリセルが選択される。こうして、メモリセルには、暗号化処理装置７００３により暗号化されたデータが書き込まれる。

【０３０１】

また、メモリセルアレイからのデータの読み込みは、、次のような動作である。アドレスバス７００８で指定されたアドレスが、アドレスデコーダ７００５によりでコードされ、ワード選択信号としてメモリセルアレイ７００２に送られる。そして、ワード選択信号によって選択されたメモリセルの内容が読み出される。読み出されたメモリセルの内容は、複号化装置７００４に送られる。複号化装置７００４は、暗号鍵記憶装置（鍵バッファ）７００６内の情報とアドレスバス７００８の情報を、ＥＯＲ回路７１０９で合成して得られる暗号鍵を用いて、メモリセルから読み出された内容を複号化する。こうして、復号化されたデータはデータバス７００７に出力する。

【０３０２】

このように、データバス７００７から送られてきたデータをメモリセルアレイ７００２に格納する前に暗号化が施され、一方、メモリセルアレイからデータを読み出す際には複号化が施されてデータバス７００７に出力される。従って、半導体記憶装置は普通の情報記憶装置と同等に扱える。　この結果、セル上に記録されるデータのビットパタンは記憶させようとしたデータとは異なるため、セル上のデータの書き込み・読み込み時の消費電流パタンからセル上の実際のデータが容易に推測する事が困難になる。

【０３０３】

図３４は発明の第２５の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置の例である。本例は暗号化に当って、暗号化鍵を用いるが、この暗号化鍵を自動初期化するものである。

【０３０４】

本実施例の情報記憶装置は、図３１の実施例の暗号鍵記憶装置７００６に、暗号化鍵自動初期化装置７２１０を接続し、この暗号化鍵自動初期化装置７２１０で暗号鍵を初期化するようにしたものである。本例のその他の構成は前述の例と同様であるので、その詳細説明は省略する。

【０３０５】

暗号化鍵自動初期化装置７２１０は、通例の乱数発生装置を使用して、初期値

を設定する構成になっている。情報処理装置が起動もしくはリセットスタートした際に、暗号化鍵自動初期化装置７２１０は、乱数により暗号鍵を自動生成し、暗号鍵記憶装置７００６に暗号鍵を設定する。このことにより、起動もしくはリセットスタートのたびに暗号鍵が変更され、同一のデータを格納した場合でも、起動毎にセル上のデータの書き込み、読み込み時の消費電流パタンが変化する。従って、消費電流パタンからセル上の実際のデータが容易に推測する事が困難になる。

【０３０６】

図３５は発明の第２６の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置の例である。本例は暗号化に当って、暗号化を行うか否かを制御を行なうものである。

【０３０７】

本実施例の情報記憶装置は、メモリセルアレイ７００２、アドレスデコーダ７００５、暗号化装置７００３、複号化装置７００４、暗号鍵記憶装置７００６、暗号化領域指定レジスタ７３１１、暗号化判定回路７３１２を有する。ここで、メモリセルアレイ７００２の構成は、通例に従って十分である。

【０３０８】

メモリアレイ７００２はアドレス値によって複数の領域に分類され、それぞれの領域に対して暗号化を行うか否かを、暗号化領域指定レジスタ７３１１で指定する。暗号化判定回路７３１２は、アドレスバス７００８に現れるアドレス値と、暗号化領域指定レジスタ７３１１の値によって、暗号化を行うか判定する。

【０３０９】

図２０に、本例で用いる暗号化判定回路のひとつの実施例を示す。この例は前述したものと同様である。この暗号化判定回路の実施例では、メモリを分割する際の上位ｐビット分を参照し、メモリアレイの領域をｐビットのそれぞれの状態で識別し、２＾ｐの領域に分割する。暗号化領域指定レジスタ７３１１は、２＾ｐビットの長さを持ち、各ビットはメモリアレイ上の１つの領域と対応し、暗号化を行うか否かを制御する。

【０３１０】

暗号化領域指定レジスタ７３１１の各ビットと、当該ビットに相当するアドレス領域を表すビットパタンに対して、ビットがすべて１となるようにＮＯＴを挟んだのち、暗号化領域指定レジスタの該当ビットとの論理積をとる。この論理積が１のときは、暗号化を行い、０の時は暗号化を行わない。暗号化領域指定レジスタ７３１１の各ビットに対して同様の回路を作り、その後論理積すべてのビットの論理和をＯＲ回路７３１４で取る。この論理和が１のときは、暗号化を行い、０の時は暗号化を行わないようにする。

【０３１１】

つぎに、暗号化判定回路７３１２の出力と、暗号鍵のＡＮＤを論理積演算装置７３１３で論理積を計算する。論理積演算装置７３１３の出力は、暗号化を行う際には、暗号鍵と同じ値になるが、暗号化を行わないときには、０を出力する。暗号化装置７００３は、暗号鍵として０が与えられると、入力と出力が等しくなるので、暗号化を行わないのと等価になる。

【０３１２】

読み出し事の複号化の手順は、書き込みと同様、アドレスの値と暗号化領域指定レジスタ７３１１の値によって、複号化を行う際の暗号鍵を０とするか暗号鍵の値にするかを制御し、複号化を行う。

【０３１３】

このようにして、メモリセルアレイをアドレスによって複数領域に分割して、それぞれの領域ごとに暗号化の有無が設定できる。暗号化を施された領域では、セル上に記録されるデータのビットパタンは記憶させようとしたデータとは異なるため、セル上のデータの書き込み、読み込み時の消費電流パタンからセル上の実際のデータが容易に推測する事が困難になる。

【０３１４】

第２７の実施の形態より第２８の実施の形態はいわゆる半導体記憶装置とその他の情報処理装置を一つの装置内に有する例である。

【０３１５】

図３６は発明の第２７の実施の形態を説明する為の情報処理装置の基本構成図

である。

【０３１６】

本例では、情報記憶装置７０５２には予め暗号化されたデータが格納されているものとして、これ以降の動作を説明する。尚、この暗号化されたデータの格納は、これまでに説明した諸方法によって行うことが出来る。　本実施例の情報記憶装置は、データ処理装置７０５１、情報記憶装置７０５２がデータバス７０５７でつながれている。そして、データ処理装置７０５１とデータバス７０５７の間に複号化装置７０５３および複号化装置で暗号を複号化するための鍵情報を格納した鍵バッファ７０５６が設けられている。

【０３１７】

ここで、復号化装置、鍵バッファ自体はこれまで説明したもので十分である。

【０３１８】

尚、前述したように、情報記憶装置７０５２には、複号化装置７０５３と鍵バッファ７０５６に格納された暗号化鍵により復号できる形式で暗号化された情報が予め格納されている。暗号化された情報は、データバス７０５７により複号化装置７０５３に送られ、複号化装置７０５３により複号化される。そして、復号化されたデータが複号化装置７０５３よりデータ処理装置７０５１に送られる。

【０３１９】

従って、情報記憶装置や信号線を流れる情報は、データ処理装置で使用される情報とは異なるビットパタンを有しており、情報記憶装置７０５２やデータバス７０５７での消費電流パタンから情報を推測する事が困難となる。

【０３２０】

図３７は発明の第２８の実施の形態を説明する為の情報処理装置の基本構成図である。本例はデータの復号化に当って、暗号化鍵を用いる例である。

【０３２１】

本例では、情報記憶装置７０５２には予め暗号化されたデータが格納されているものとして、これ以降の動作を説明する。尚、この暗号化されたデータの格納は、これまでに説明した諸方法によって行うことが出来る。　本実施例の情報記憶装置は、データ処理装置７０５１、情報記憶装置７０５２がデータバス７０５

７でつながれている。そして、データ処理装置７０５１とデータバス７０５７の間に複号化装置７０５３および複号化装置で暗号を複号化するための鍵情報を格納した鍵バッファ７０５６、およびアドレスバス７０５８が設けられている。ここで、復号化装置、鍵バッファ自体はこれまで説明したもので十分である。

【０３２２】

複号化装置７０５３は、複号化する際の暗号化鍵として、情報記憶装置７０５２の格納アドレスの一部分と、鍵バッファ７０５６に格納された暗号鍵とのＥＯＲを計算したものを暗号化鍵として使用する。情報記憶装置７０５２には、複号化装置７０５３により復号可能な形式で暗号化された情報が予め格納されている。

【０３２３】

データ処理装置７０５１がアドレスバス７０５８にアドレス情報を出力すると、情報格納装置７０５２は、データバスに暗号化された状態のデータをそのままデータバス７０５７に出力する。複号化装置７０５３には、情報記憶装置７０５２の格納アドレスの一部分と、鍵バッファ７０５６に格納された暗号鍵とのＥＯＲをＥＯＲ回路７０５４により計算された複号化鍵が暗号化された情報とが、鍵として送られる。そして、この鍵によって、データバス７０５７上の情報を複号化して、データ処理装置７０５１へ送る。

【０３２４】

この場合、情報記憶装置７０５２やデータバス７０５７を流れる情報は、データ処理装置７０５１で使用される情報とは異なるビットパタンを有している。又、格納アドレスごとに暗号化の鍵情報が異なるため、消費電力が同じ値であっても、アドレスによって異なるビットパタンに暗号化されている。この為、情報記憶装置や信号線でのの消費電流パタンから情報を推測する事が前記第２７の実施の形態に係る発明よりも更に困難となる。　図３８は発明の第２９の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置とその他の情報処理装置を有する例である。

【０３２５】

本実施例の情報記憶装置は、データ処理装置７０５１、情報記憶装置７０５２

がデータバス７０５７でつながれている。そして、データ処理装置７０５１とデータバス７０５７の間に複号化装置７０５３および複号化装置で暗号を複号化するための鍵情報を格納した鍵バッファ７０５６、およびアドレスバス７０５８が設けられている。更に、記憶領域のどの領域のデータを暗号化するかを指定する為に、ＡＮＤ回路１１１２、暗号化領域指定レジスタ７３１１、暗号化判定回路７３１２を有する。ここで、情報記憶装置７０５２の構成は、通例に従って十分である。又、復号化装置、鍵バッファ自体など個別の手段は、例えばこれまで説明したもので十分である。

【０３２６】

本実施の形態に特徴的な暗号化領域の指定に関する動作を主に説明する。

【０３２７】

それぞれの記憶領域に対して暗号化を行ったか否かを、暗号化領域指定レジスタ７３１１で指定する。暗号化判定回路７３１２は、アドレスバス７０５８に現れるアドレス値と、暗号化領域指定レジスタ７３１１の値によって、復号化を行うか判定する。暗号化判定回路の構成は、前述の図２０と同一である。情報記憶装置７０５２には、複号化装置７０５３により復号可能な形式で暗号化された情報が予め格納されている。データ処理装置７０５１がアドレスバス７０５８にアドレス情報を出力すると、情報格納装置７０５２は、データバスに暗号化された状態のデータを出力する。暗号化判定回路７３１２は、アドレスバス７０５８に出力されたアドレス値の一部と、暗号化領域指定レジスタ７３１１の値を参照して、該アドレスのデータが暗号化されているか否かを判定し、暗号化されている場合は１を、暗号化されていない場合は０を返す。

【０３２８】

暗号化判定回路７３１２の出力は、ＡＮＤ回路１１１２にて鍵バッファ７０５６とＡＮＤが取られる。その結果、複号化装置７０５３には、暗号化されているアドレス領域をアクセスした場合は、鍵バッファ７０５６の内容が渡り、暗号化されていないアドレス領域をアクセスした場合は、０が渡る。複号化装置７０５３はＥＯＲ回路になっているため、０が渡されると入力された値をそのままデータ処理装置７０５１へ渡す。したがって、暗号化された領域のデータは鍵バッフ

ァ７０５６の値を用いて正しく複号化される一方、暗号化されていない領域のデータはそのままデータ処理装置７０５１に渡される。暗号化を施された領域では、データバス７０５７に現れるビットパタンや情報記憶装置７０５２に記録されるデータのビットパタンは実際のデータとは異なるため、情報記憶装置７０５２の読み込み時の消費電流パタンやデータバス７０５７で消費される電流パタンから実際のデータを推測する事が困難となる。

【０３２９】

図３９は発明の第３０の実施の形態を説明する為の情報処理装置の基本構成図である。本例はいわゆる半導体記憶装置とその他の情報処理装置を有する半導体装置システムの例である。

【０３３０】

本実施例のランダム転送制御装置は、転送元のアドレスを記憶するアドレスレジスタ１８００２と、転送先のアドレスを記憶するアドレスレジスタ１８００３と、転送元、転送先レジスタを切り替えるためのマルチプレクサ１８００４と、転送先、転送元アドレスレジスタの値を更新するための加算器１８００５と、アドレスレジスタと乱数とＥＯＲを取り、転送アドレスの転送順番をランダム化するための排他的論理和演算装置１８００７と、排他的論理和演算装置１８００７で転送順番を変えるための排他的論理和演算に用いる乱数値を生成するための乱数発生装置１８００６と、転送回数をカウントするためのカウンタ１８００９と、順番を変えて生成されたアドレスを一時的に保管するアドレスバッファ１８００８と、転送されるデータを一時的に保管するデータバッファ１８０１１、転送順番をランダムかしたときのアドレスを保存するアドレスレジスタ、これらの各回路を制御して転送を実行する制御回路１８０１２とにより構成されている。まず転送元アドレスが転送元アドレスレジスタ１８００２に、転送先アドレスが転送先アドレスレジスタ１８００３に、転送バイト数がカウンタ１８００９にセットされる。ここで、カウンタにセットされる転送バイト数の初期値は２の累乗の値をとる。転送元アドレスレジスタ１８００２転送先アドレスレジスタ１８００３、に初期値としてセットされる値は、転送バイト数で余剰を計算したときに、０となる値である必要がある。次に、制御装置１８０１２の転送動作を順を追っ

て説明する。

【０３３１】

ＳＴＥＰ ０：まず制御回路１８０１２から乱数発生回路１８００６へ乱数発生要求が送られ、乱数発生回路１８００６では、転送前に転送バイト数よりも小さな値の乱数を生成し保持する。

【０３３２】

ＳＴＥＰ １：つぎに、制御回路８０１２からマルチプレクサ１８００４に対して、転送元アドレスレジスタ１８００２を選択するように選択信号が送られ、マルチプレクサをとおった転送元アドレスは、乱数発生回路１８００６に保持された乱数値との排他的論理和演算を排他的論理和演算装置１８００７で行い、アドレスバッファ１８００８に格納される。

【０３３３】

ＳＴＥＰ ２：制御回路１８０１２は、アドレスバッファ１８００８のアドレス値をアドレスバスに出力し、アドレスバス１８０３２に乗ったアドレス値の内容がデータバス１８０３１に載ったのち、制御回路１８０１２は、ラッチ信号をデータバッファ１８０１１に送って、データバッファ１８０１１にデータバスの値を格納する。加算回路１８００５では、転送元アドレスレジスタの値に１を加算する計算が行われている。加算が終わったら、制御回路１８０１２から転送元アドレスレジスタに対するラッチ信号を制御して、転送元アドレスレジスタに加算回路の出力を格納する。

【０３３４】

ＳＴＥＰ３：つぎに、制御回路１８０１２は制御回路１８０１２からマルチプレクサ１８００４に対して、転送先アドレスレジスタ１８００３を選択するように選択信号が送られ、マルチプレクサをとおった転送先アドレスは、乱数発生回路１８００６に保持された乱数値とのＥＯＲ演算をＥＯＲ回路１８００７で行い、アドレスバッファ１８００８に格納される。

【０３３５】

ＳＴＥＰ ４：制御回路１８０１２は、アドレスバッファ１８００８のアドレス値をアドレスバス１８０３２へ、データバッファ１８０１１のデータ値をデータ

バス１８０３１に出力するように制御信号を送る。さらにアドレスバス１８０３２のアドレスに、データバス１８０３１上のデータを書き込むように制御信号を発行する。

【０３３６】

ＳＴＥＰ ５：加算回路１８００５では、転送先アドレスレジスタの値に１を加算する計算が行われている。加算が終わったら、制御回路１８０１２は転送先アドレスレジスタ１８００３に対するラッチ信号を制御して、転送先アドレスレジスタ１８００３に加算回路１８００５の出力を格納する。

【０３３７】

ＳＴＥＰ ６：カウンタ１８００９の値に-１を加算回路１８０１０で加算し、１減算する。制御回路１８０１２は、カウンタ１８００９へラッチ信号を送り、加算回路１８０１０の演算結果をカウンタ１８００９に格納する。

【０３３８】

ＳＴＥＰ ７：つぎに制御回路は、カウンタ１８００９の内容が０か否かを検査し、非ゼロの場合は、ＳＴＥＰ １からの処理を繰り返す。

【０３３９】

以上の動作により、乱数値の違いにより、同一の内容を同一のアドレスに対して転送する場合でも、乱数発生回路で生成される乱数値が異なることで、データの転送順が異なり、動作時の消費電流パタンが毎転送ごとに異なることとなり、消費電流パタンから同一のデータを転送しているか否かを推測する事が困難になる。

【０３４０】

【発明の効果】

本願発明は、高いセキュリティを持つ情報処理装置を提供することが出来る。本願発明は、高いセキュリティを持つ情報記憶装置を提供することが出来る。更には、本願発明は、高いセキュリティを持つカード部材、および情報処理システムを提供することが出来る。

【図面の簡単な説明】

【図１】

図１はマイクロコンピュータの基本構成を示す図である。

【図２】

図２はＩＣカードにおける半導体集積回路装置の配置を示す図である。

【図３】

図３はカード・システムの概要を示す構成図である。

【図４】

図４は通例のＩＣカード用半導体装置における１サイクルの消費電力を示す電流波形を示す図である。

【図５】

図５は本願情報処理装置の第１の実施の形態を示す基本構成図である。

【図６】

図６はデータの一時記憶の為のフリップフロップの例を示す図である。

【図７】

図７は信号線の状態と電力消費の為のコンデンサの状態を示す図であり、同図の（ａ）はプリチャージ方式の場合、同図の（ｂ）はスタティック方式の場合の諸例を示すものである。

【図８】

図８は本願情報処理装置の第２の実施の形態を示す基本構成図である。

【図９】

図９は本願情報処理装置の第２の実施の形態の別な例を示す基本構成図である。

【図１０】

図１０は本願情報処理装置の第３の実施の形態を示す基本構成図である。

【図１１】

図１１は本願情報処理装置の第４の実施の形態を示す基本構成図である。

【図１２】

図１２は本願情報処理装置の第５の実施の形態を示す基本構成図である。

【図１３】

図１３は本願情報処理装置の第６の実施の形態を示す基本構成図である。

【図１４】

図１４は本願情報処理装置の第７の実施の形態を示す基本構成図である。

【図１５】

図１５は本願情報処理装置の第８の実施の形態を示す基本構成図である。

【図１６】

図１６は本願情報処理装置の第９の実施の形態を示す基本構成図である。

【図１７】

図１７は本願情報処理装置の第１０の実施の形態を示す基本構成図である。

【図１８】

図１８は本願情報処理装置の第１１の実施の形態を示す基本構成図である。

【図１９】

図１９は本願情報処理装置の第１２の実施の形態を示す基本構成図である。

【図２０】

図２０は暗号化判定回路の一例を示す図である。

【図２１】

図２１は本願情報処理装置の第１３の実施の形態を示す基本構成図である。

【図２２】

図２２は本願情報処理装置の第１４の実施の形態を示す基本構成図である。

【図２３】

図２３は本願情報処理装置の第１５の実施の形態を示す基本構成図である。

【図２４】

図２４は本願情報処理装置の第１６の実施の形態を示す基本構成図である。

【図２５】

図２５は本願情報処理装置の第１７の実施の形態を示す基本構成図である。

【図２６】

図２６は本願情報処理装置の第１８の実施の形態を示す基本構成図である。

【図２７】

図２７は本願情報処理装置の第１９の実施の形態を示す基本構成図である。

【図２８】

図２８は本願情報処理装置の第２０の実施の形態を示す基本構成図である。

【図２９】

図２９は本願情報処理装置の第２１の実施の形態を示す基本構成図である。

【図３０】

図３０は本願情報処理装置の第２２の実施の形態を示す基本構成図である。

【図３１】

図３１は本願情報処理装置の第２３の実施の形態を示す基本構成図である。

【図３２】

図３２はメモリセルアレーのひとつの例を示す図である。

【図３３】

図３３は本願情報処理装置の第２４の実施の形態を示す基本構成図である。

【図３４】

図３４は本願情報処理装置の第２５の実施の形態を示す基本構成図である。

【図３５】

図３５は本願情報処理装置の第２６の実施の形態を示す基本構成図である。

【図３６】

図３６は本願情報処理装置の第２７の実施の形態を示す基本構成図である。

【図３７】

図３７は本願情報処理装置の第２８の実施の形態を示す基本構成図である。

【図３８】

図３８は本願情報処理装置の第２９の実施の形態を示す基本構成図である。

【図３９】

図３９は本願情報処理装置の第３０の実施の形態を示す基本構成図である。

【図４０】

図４０は鍵バッファの実装例を示す図である。

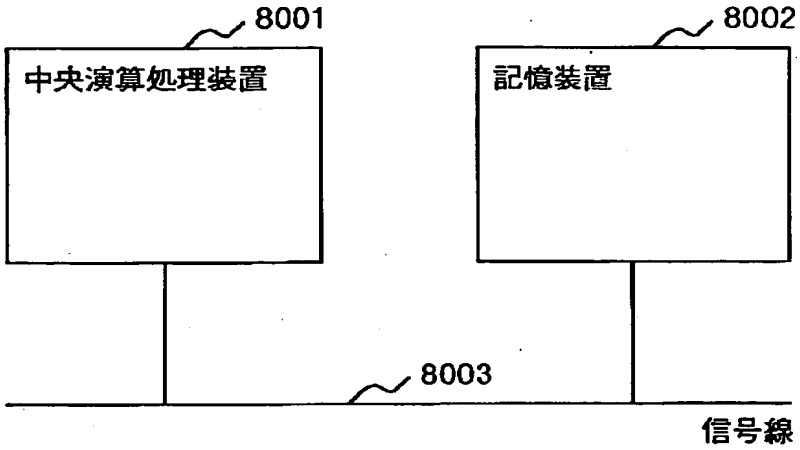
【記号の説明】

８００１は中央演算処理装置、８００２は記憶装置、５１は半導体チップ、５２はカード部材、５３はリーダライタ、５４はコントロールプロセッサ、５５は磁気ディスク、０１０１、０４０１、０５０１は情報処理装置（ＲＯＭ）、０１０２、０２０１、０２５１、０３０１、０４０２、０５０２は情報処理装置（ＣＰＵ）、０２０２、０２５２、０３０２は情報処理装置（ＲＡＭ）、１１０１、１３０１、１４０１、１５０１、１６０１、１７０１、１３０１、１４０１、１６０１、１７０１はデータ処理装置（ＣＰＵ）、１１０２、１３０２、１４０２、１５０２、１６０２、１７０２、１３０２、１４０２、１６０２、１７０２はデータ処理装置（ＲＡＭ）、０１１３、０２１３、０２６３、０３１２、０４０８、０５０６は信号線、０１１４、０１１５、０１１６、０１１７、０１１８、０１１９は電力発生装置、０３０９、０５０７はダミー信号線、０４０７、０５０５、５００８はプリチャージ信号制御装置、５００３は反転装置、５１１０１はデータ処理装置、５１１０２は情報記憶装置、５１１０７、７００７はデータバス、５１１０８、７００８はアドレスバス、７００２はメモリセルアレイである。

【書類名】図面

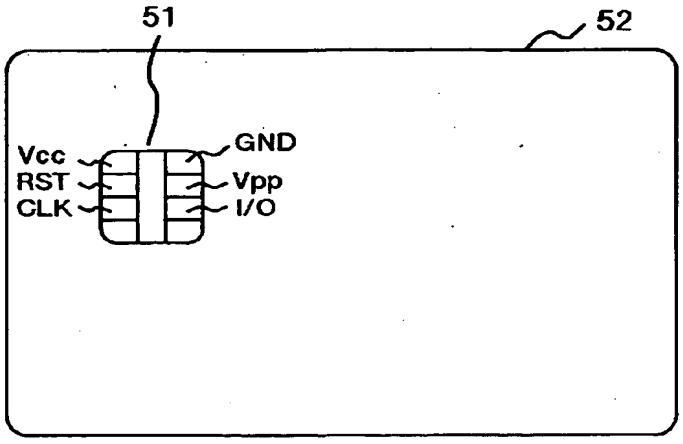
【図１】

図　1



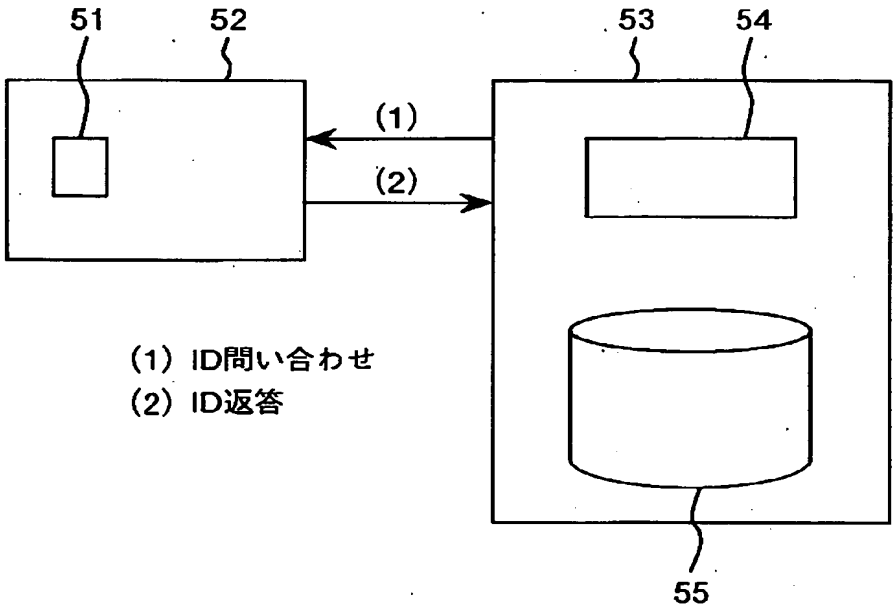
【図２】

図　2



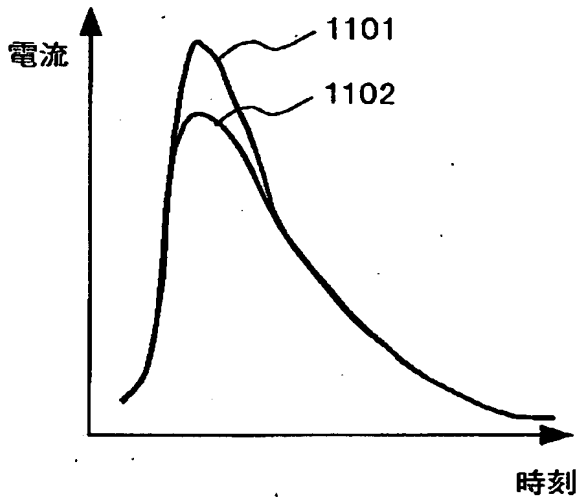
【図３】

図　3



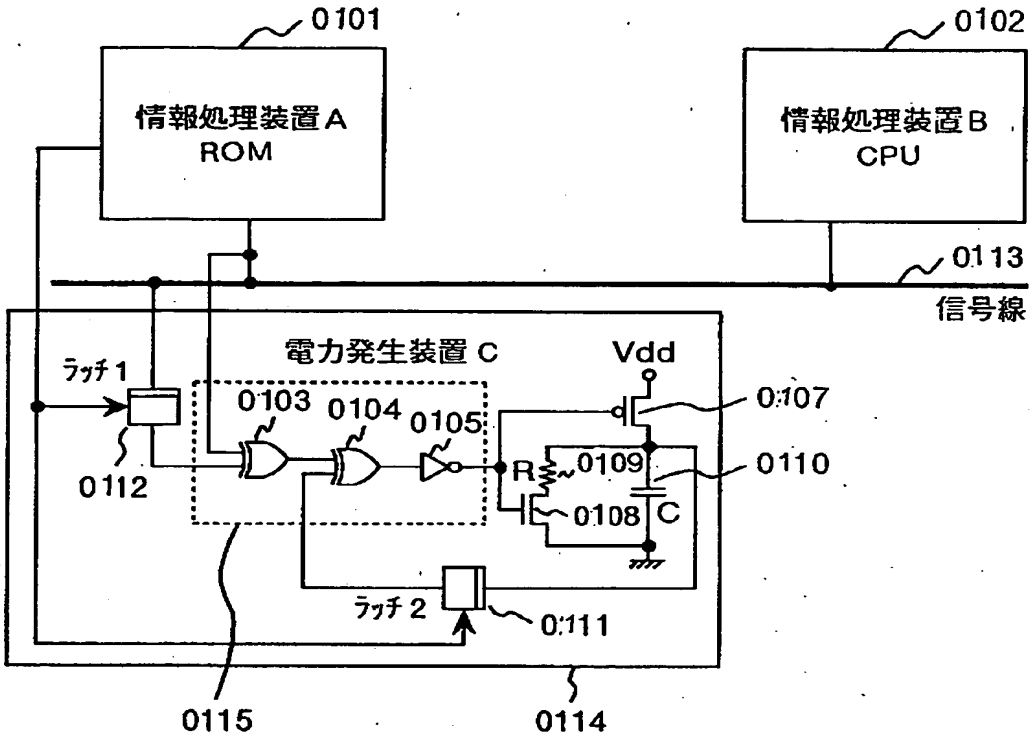
【図４】

図　4



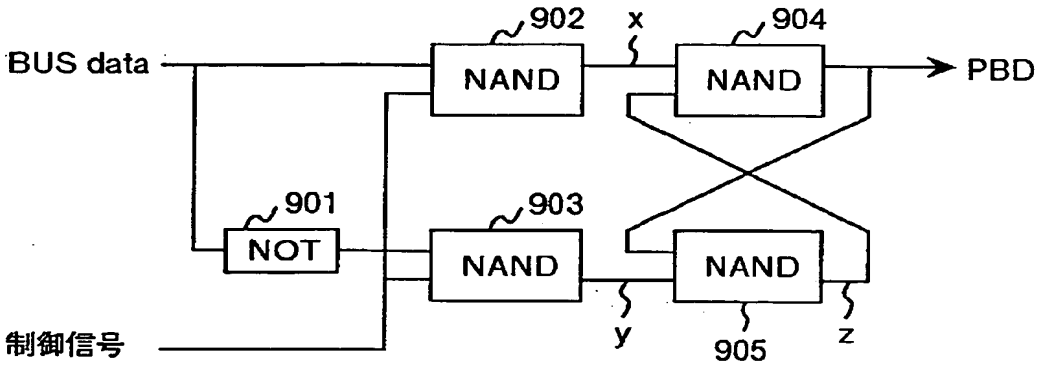
【図５】

図　５


0101
情報処理装置Ａ
ROM
0102
情報処理装置Ｂ
CPU
0113
信号線
電力発生装置Ｃ
Vdd
ﾗｯﾁ1
0103
0104
0105
0107
0110
R
0109
0108
C
0112
ﾗｯﾁ2
0111
0115
0114

【図６】

図　6

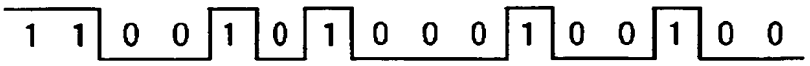

BUS data
902
x
904
NAND
NAND
PBD
901
903
NOT
NAND
NAND
制御信号
y
905
z

【図７】

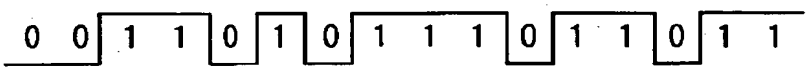
図　７

（ａ）

信号線の状態

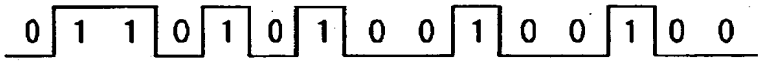


コンデンサの状態

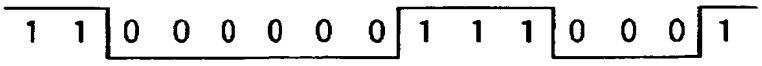


（ｂ）

信号線の状態

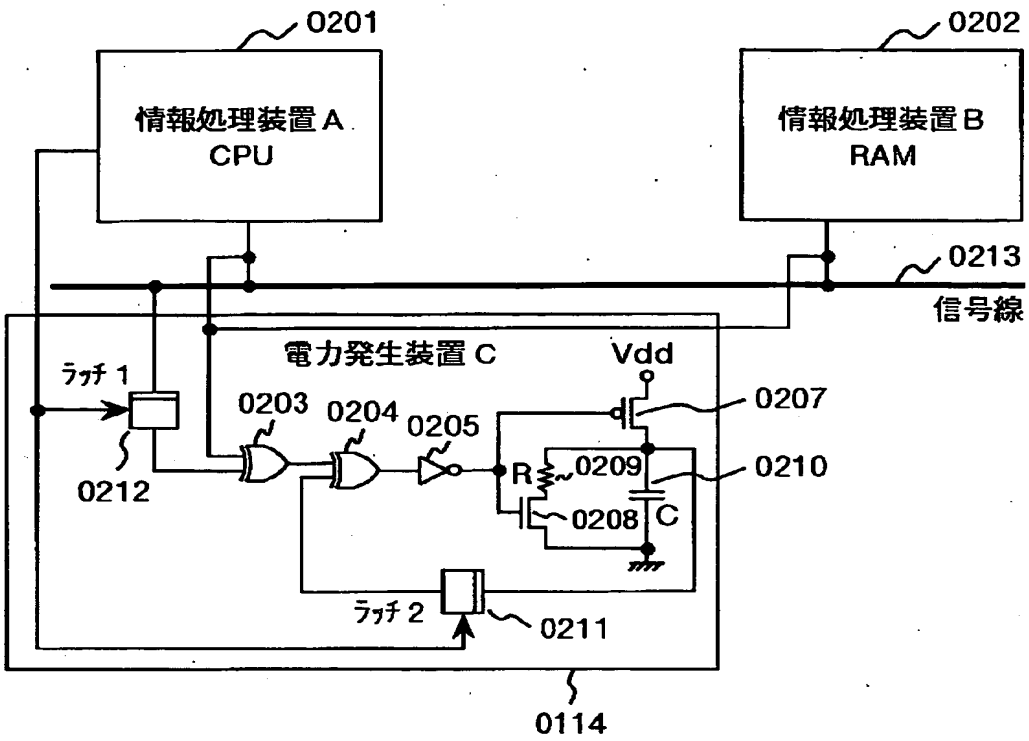


コンデンサの状態



【図８】

図　８


0201
情報処理装置Ａ
CPU
0202
情報処理装置Ｂ
RAM
0213
信号線
電力発生装置Ｃ
Vdd
ﾗｯﾁ１
0203
0204
0205
0207
0209
0210
R
0208
C
0212
ﾗｯﾁ２
0211
0114

【図９】

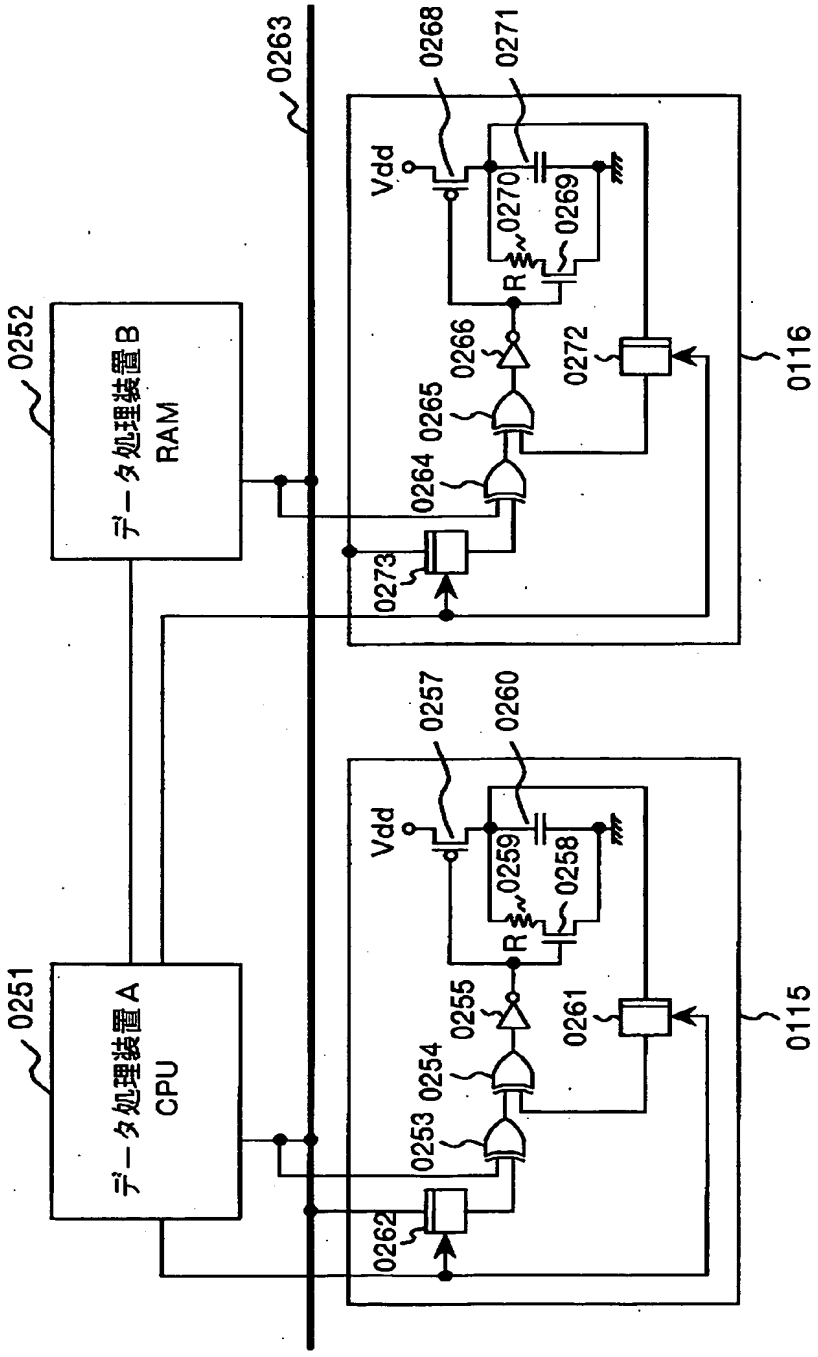

0263
0268
0271
Vdd
0270
0269
R
0252
データ処理装置B
RAM
0266
0272
0116
0265
0264
0273
0257
0260
Vdd
0259
0258
R
0251
データ処理装置A
CPU
0255
0261
0115
0254
0253
0262

図 9

【図１０】

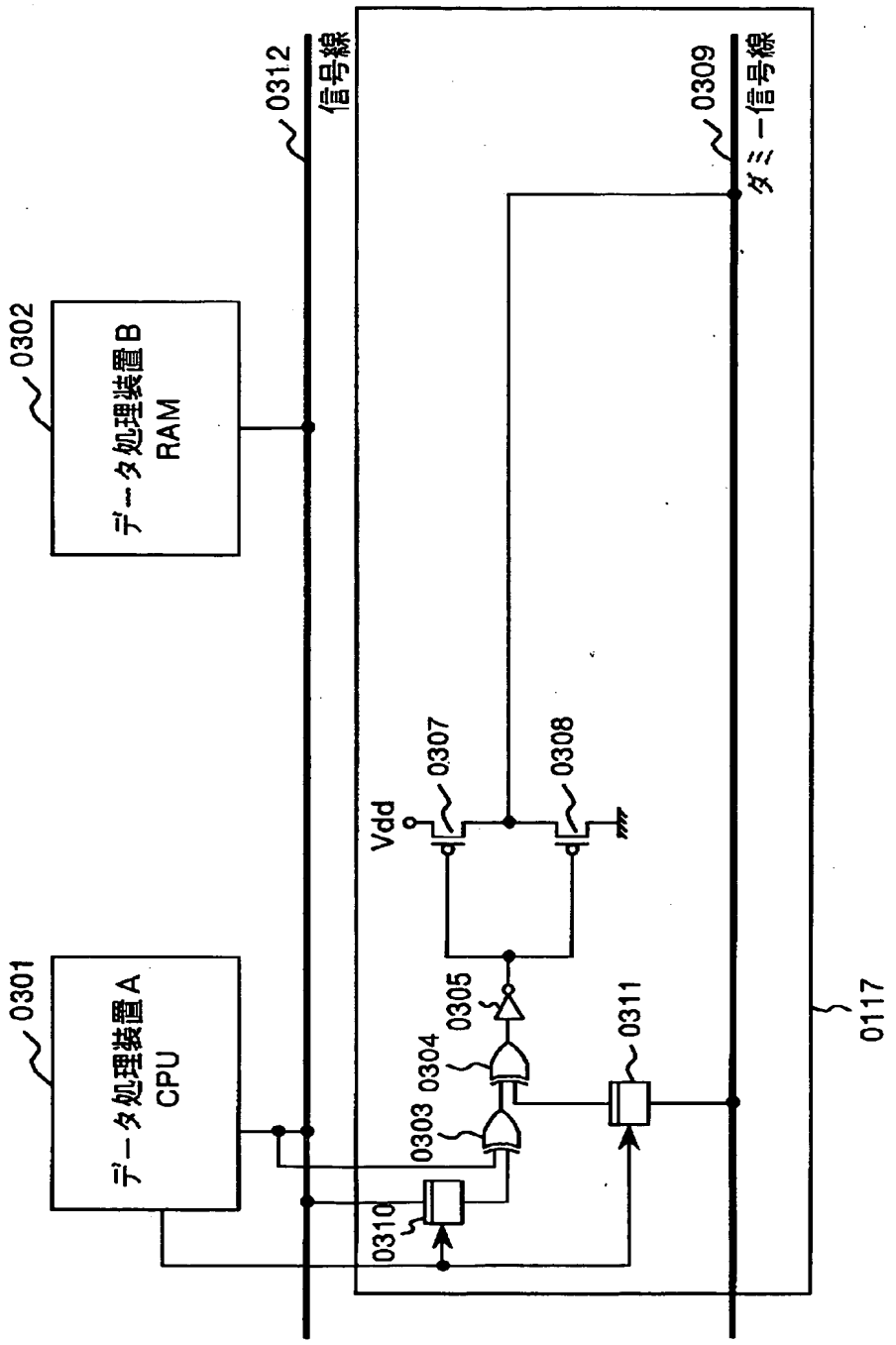
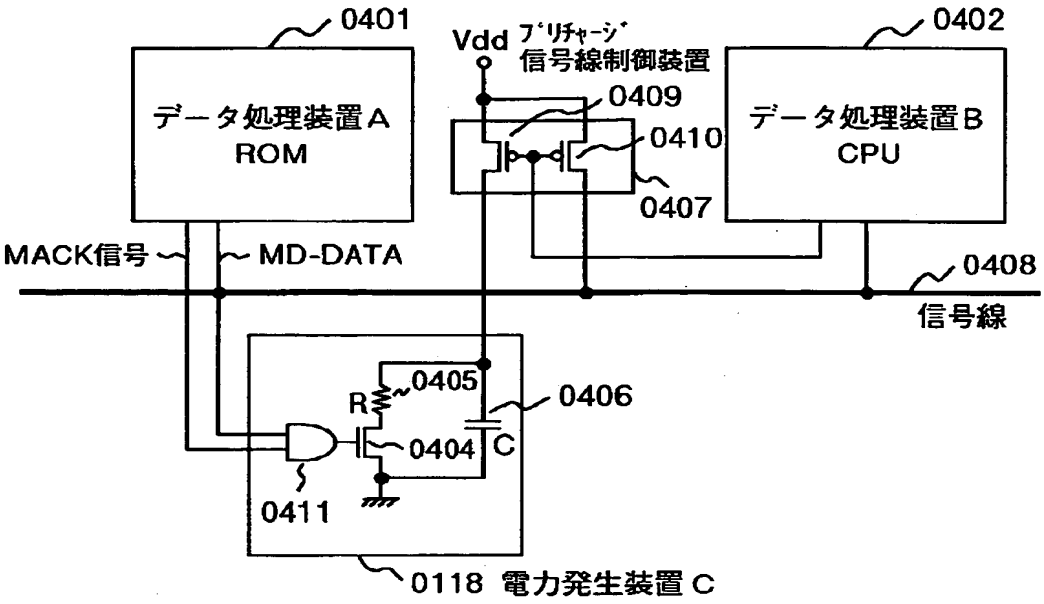

0312
信号線
0309
ダミー信号線
0302
データ処理装置B
RAM
0301
データ処理装置A
CPU
Vdd
0307
0308
0305
0304
0303
0311
0310
0117

図１０

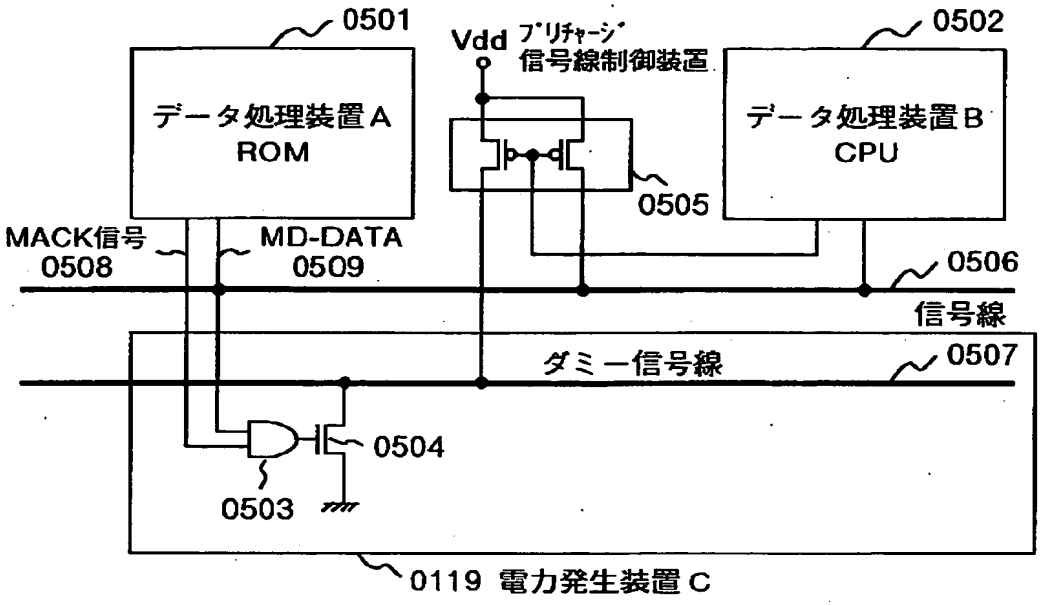
【図１１】

図　１１


0401
データ処理装置A
ROM
Vdd
プリチャージ
信号線制御装置
0409
0410
0407
0402
データ処理装置B
CPU
MACK信号
MD-DATA
0408
信号線
0405
R
0406
0404
C
0411
0118 電力発生装置C

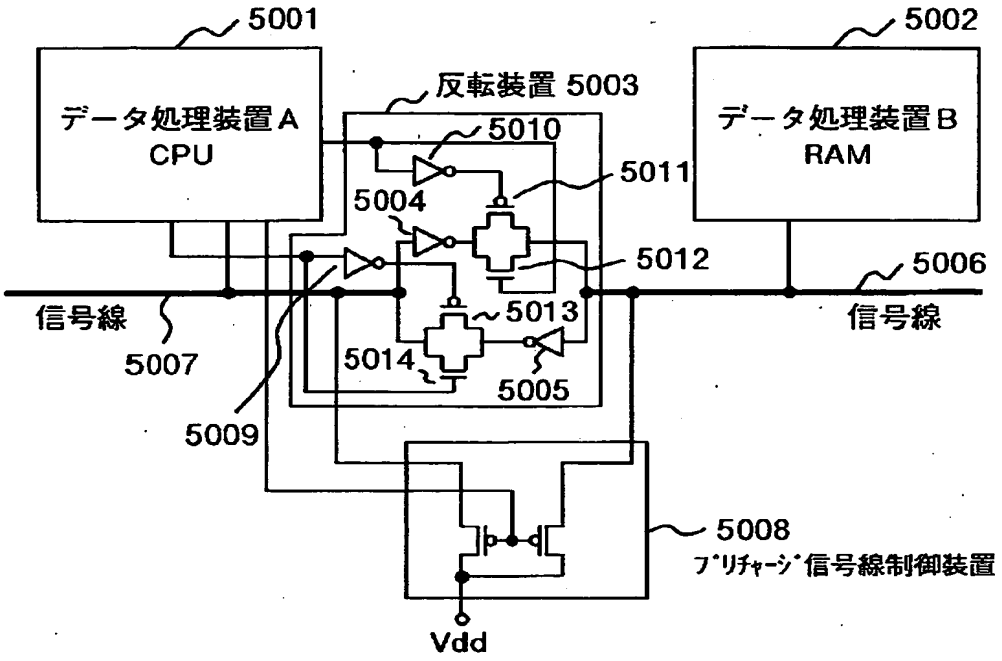
【図１２】

図　１２


0501
データ処理装置A
ROM
Vdd
プリチャージ
信号線制御装置
0502
データ処理装置B
CPU
0505
MACK信号
0508
MD-DATA
0509
0506
信号線
ダミー信号線
0507
0504
0503
0119 電力発生装置C

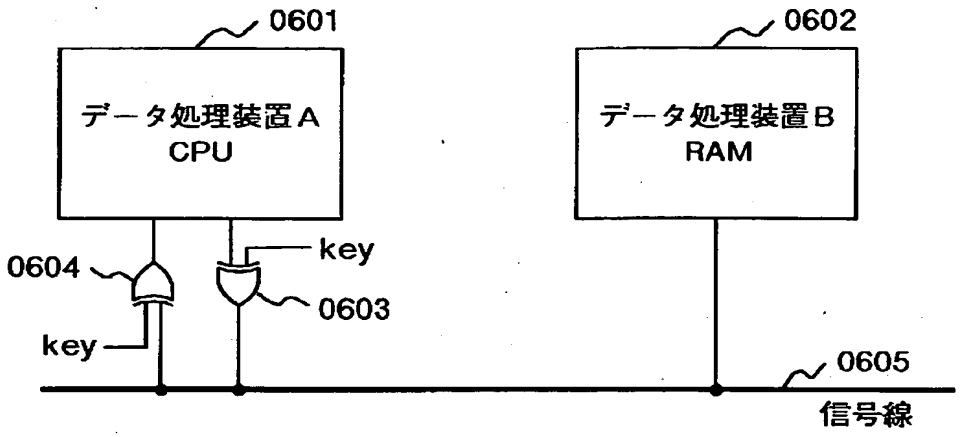
【図１３】

図　１３


5001
データ処理装置A
CPU
反転装置 5003
5010
5011
5004
5012
5002
データ処理装置B
RAM
5006
信号線
信号線
5007
5013
5014
5005
5009
5008
ﾌﾟﾘﾁｬｰｼﾞ信号線制御装置
Vdd

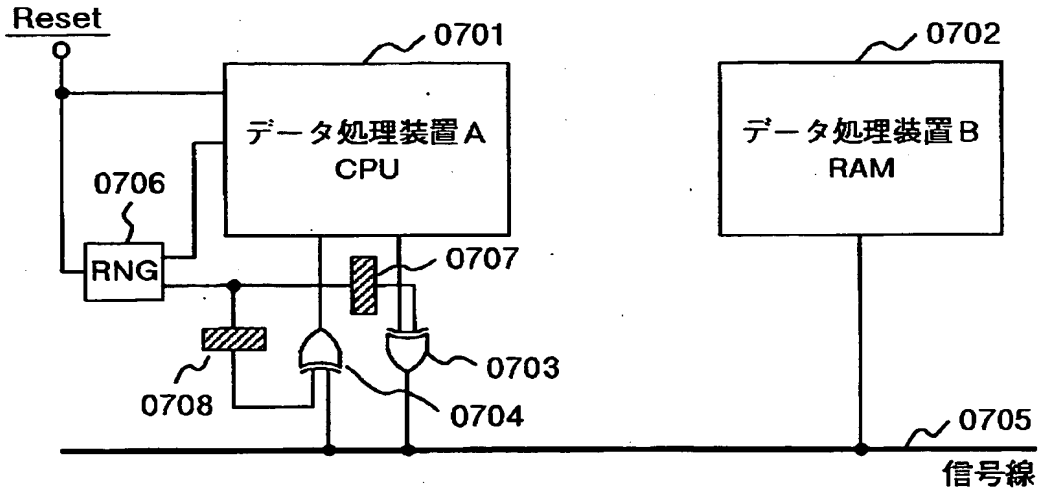
【図１４】

図　１４



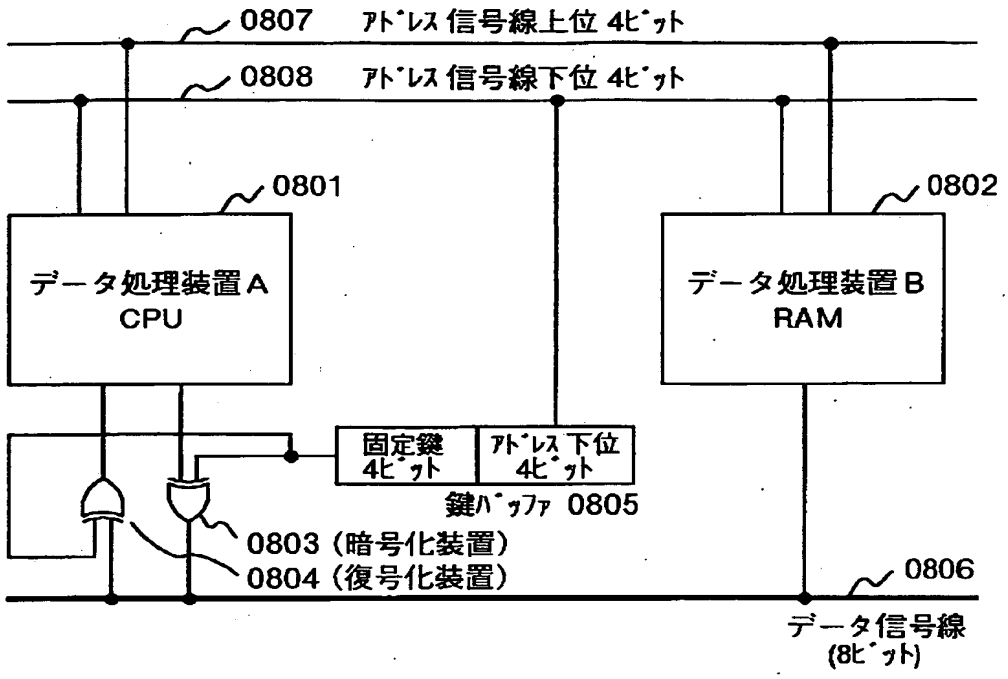
【図１５】

図　１５



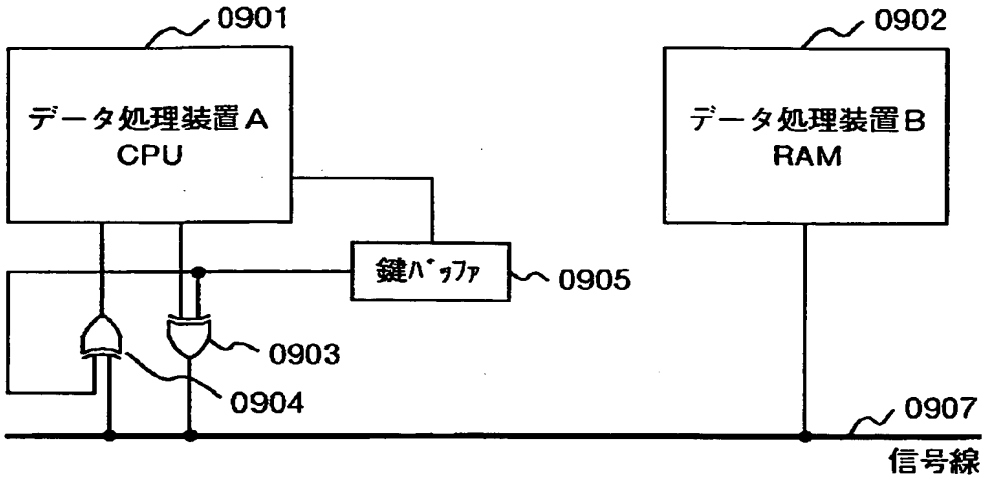
【図１６】

図　１６


0807
ｱﾄﾞﾚｽ信号線上位4ﾋﾞｯﾄ
0808
ｱﾄﾞﾚｽ信号線下位4ﾋﾞｯﾄ
0801
0802
データ処理装置A
CPU
データ処理装置B
RAM
固定鍵
4ﾋﾞｯﾄ
ｱﾄﾞﾚｽ下位
4ﾋﾞｯﾄ
鍵ﾊﾞｯﾌｧ 0805
0803（暗号化装置）
0804（復号化装置）
0806
データ信号線
(8ﾋﾞｯﾄ)

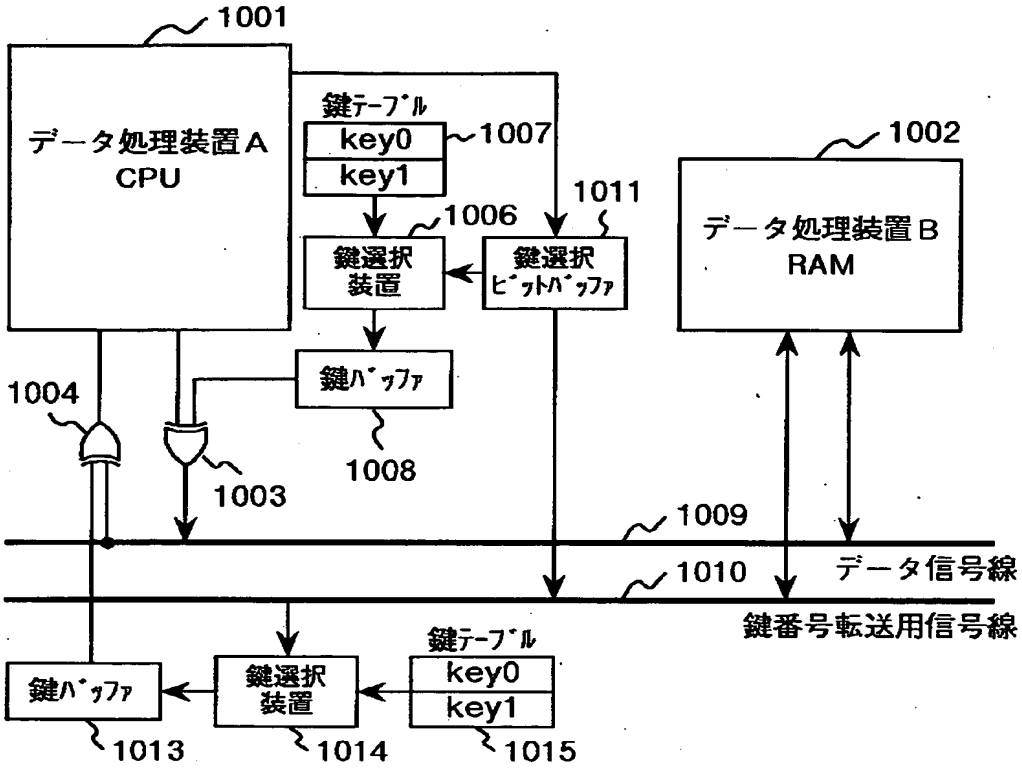
【図１７】

図　１７


0901
データ処理装置A
CPU
0902
データ処理装置B
RAM
鍵ﾊﾞｯﾌｧ
0905
0903
0904
0907
信号線

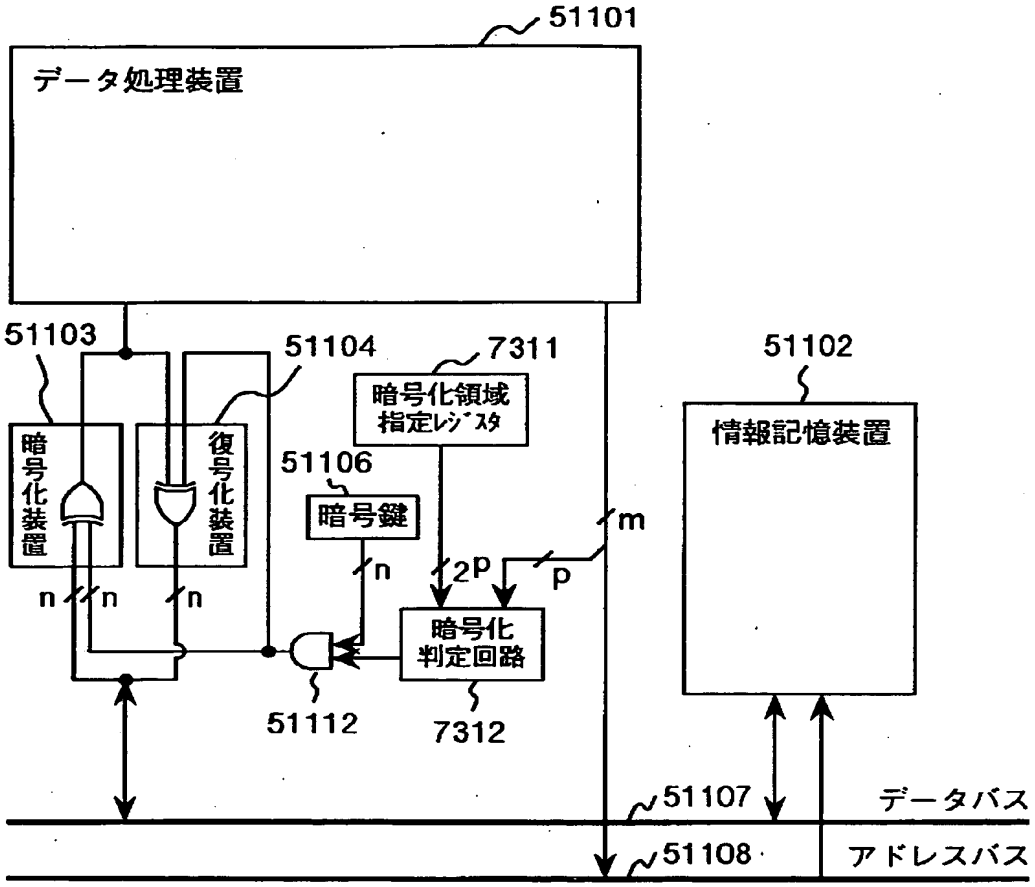
【図１８】

図　１８


1001
データ処理装置A
CPU
鍵ﾃｰﾌﾞﾙ
key0
key1
1007
1011
1006
鍵選択
装置
鍵選択
ﾋﾞｯﾄﾊﾞｯﾌｧ
1002
データ処理装置B
RAM
鍵ﾊﾞｯﾌｧ
1008
1004
1003
1009
1010
データ信号線
鍵番号転送用信号線
鍵ﾃｰﾌﾞﾙ
key0
key1
鍵ﾊﾞｯﾌｧ
鍵選択
装置
1013
1014
1015

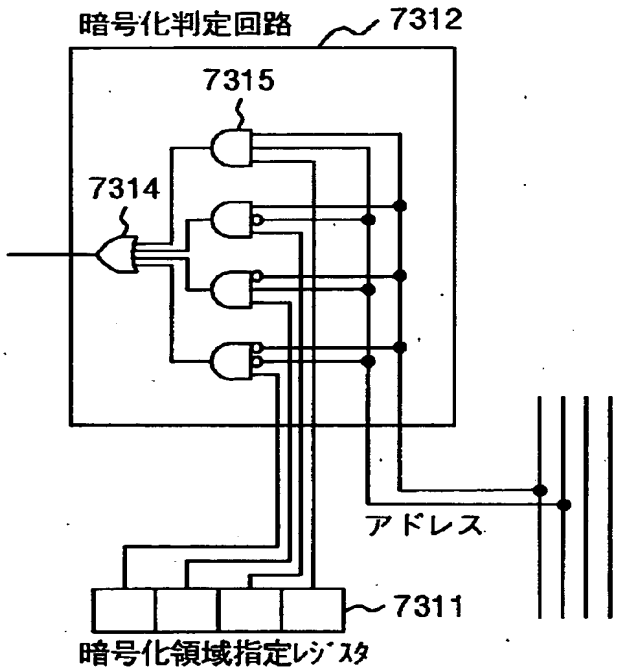
【図１９】

図　１９


51101
データ処理装置
51103
51104
7311
暗号化領域
指定レジスタ
51102
情報記憶装置
暗号化装置
復号化装置
51106
暗号鍵
m
n
2p
p
n
n
n
暗号化
判定回路
51112
7312
51107
データバス
51108
アドレスバス

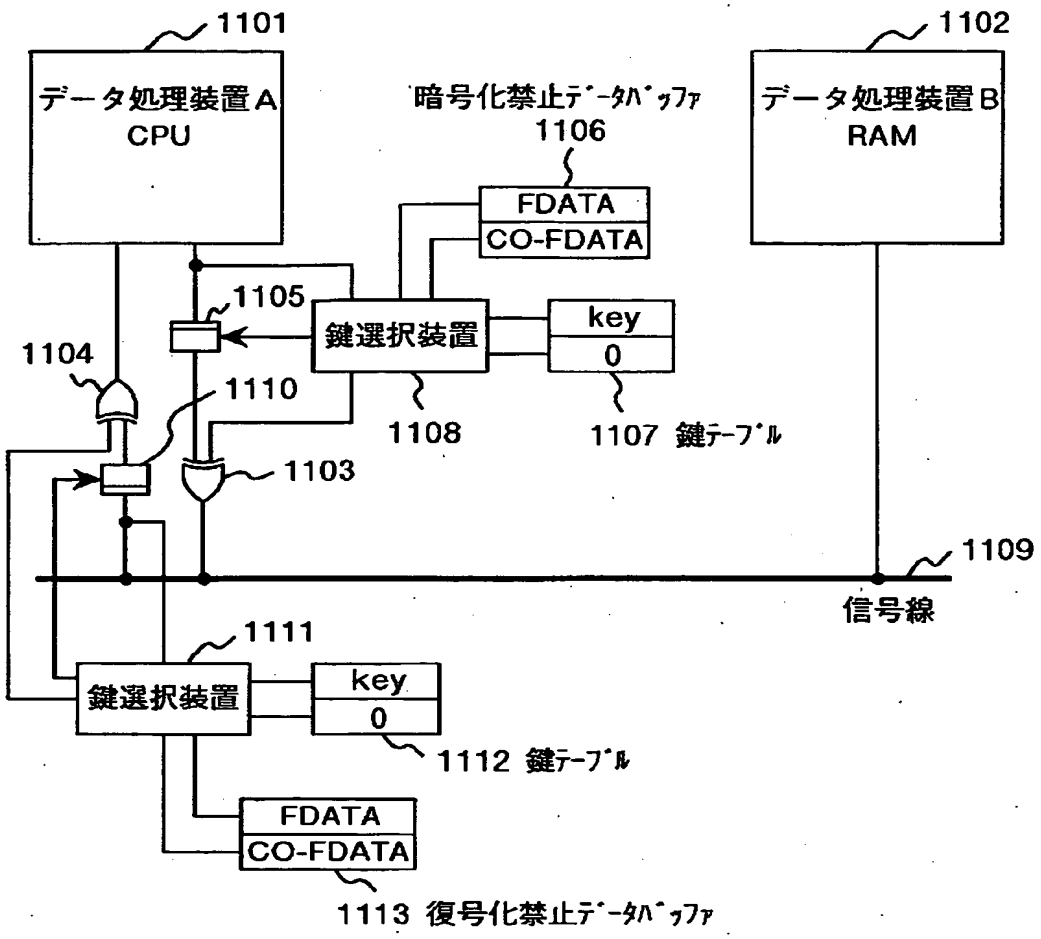
【図２０】

図　２０



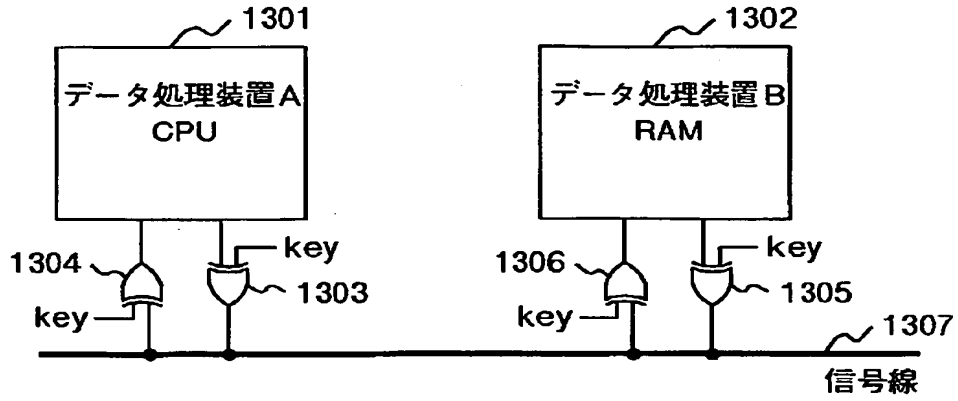
【図２１】

図　２１


1101
データ処理装置A
CPU
1102
データ処理装置B
RAM
暗号化禁止ﾃﾞｰﾀﾊﾞｯﾌｧ
1106
FDATA
CO-FDATA
1105
鍵選択装置
key
0
1104
1110
1108
1107 鍵ﾃｰﾌﾞﾙ
1103
1109
信号線
1111
鍵選択装置
key
0
1112 鍵ﾃｰﾌﾞﾙ
FDATA
CO-FDATA
1113 復号化禁止ﾃﾞｰﾀﾊﾞｯﾌｧ

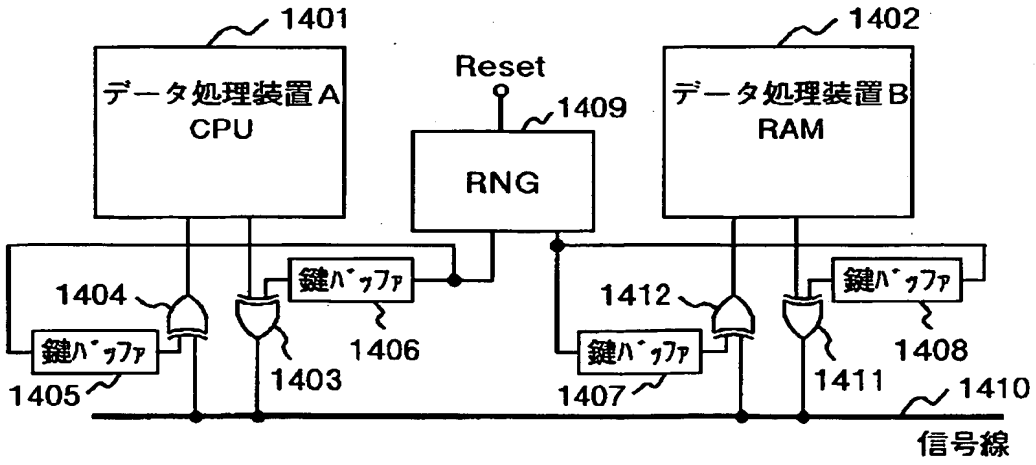
【図２２】

図　２２



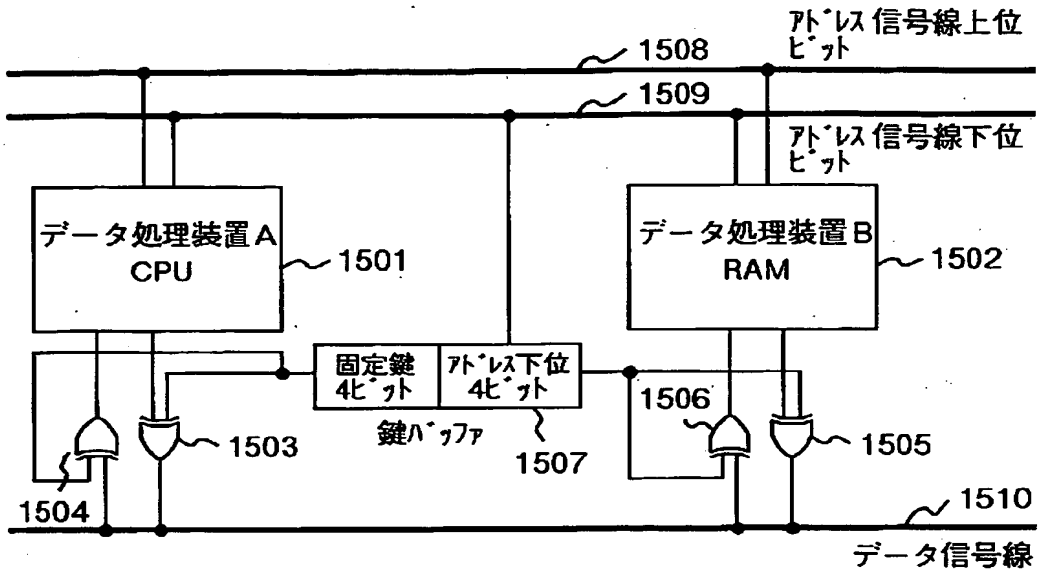
【図２３】

図　２３



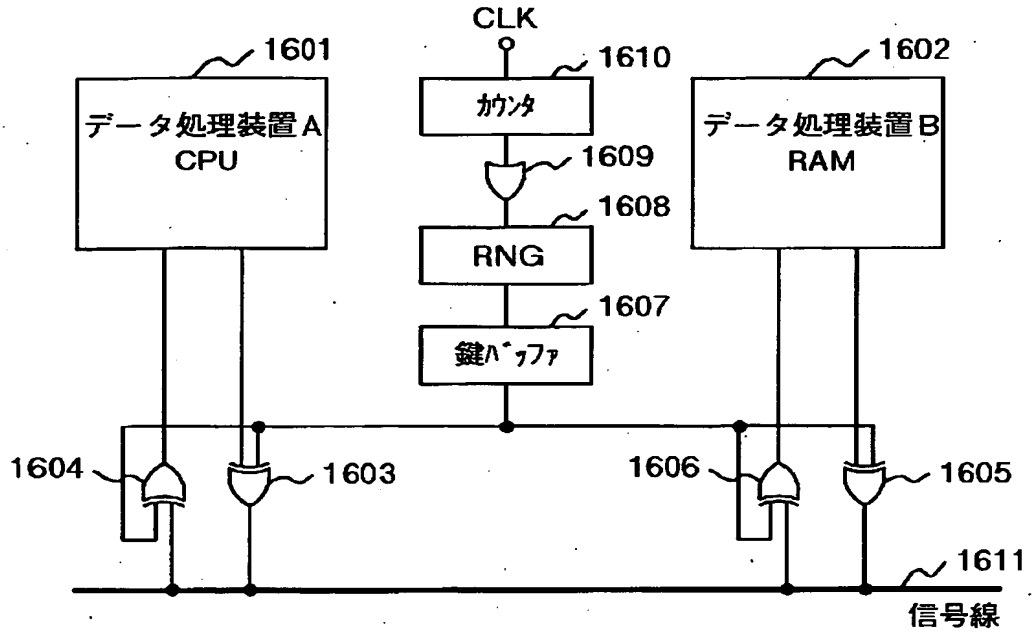
【図２４】

図　２４


ｱﾄﾞﾚｽ信号線上位ﾋﾞｯﾄ
1508
1509
ｱﾄﾞﾚｽ信号線下位ﾋﾞｯﾄ
データ処理装置A
CPU
1501
データ処理装置B
RAM
1502
固定鍵4ﾋﾞｯﾄ
ｱﾄﾞﾚｽ下位4ﾋﾞｯﾄ
鍵ﾊﾞｯﾌｧ
1507
1503
1504
1505
1506
1510
データ信号線

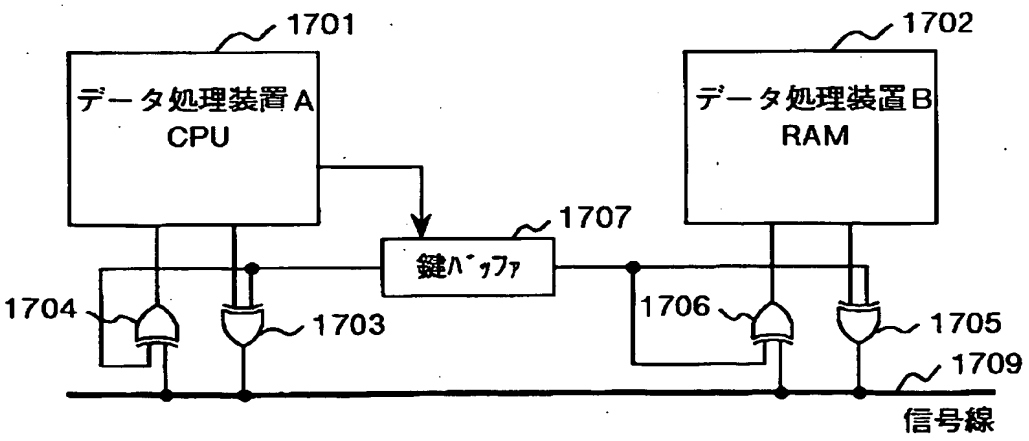
【図２５】

図　２５



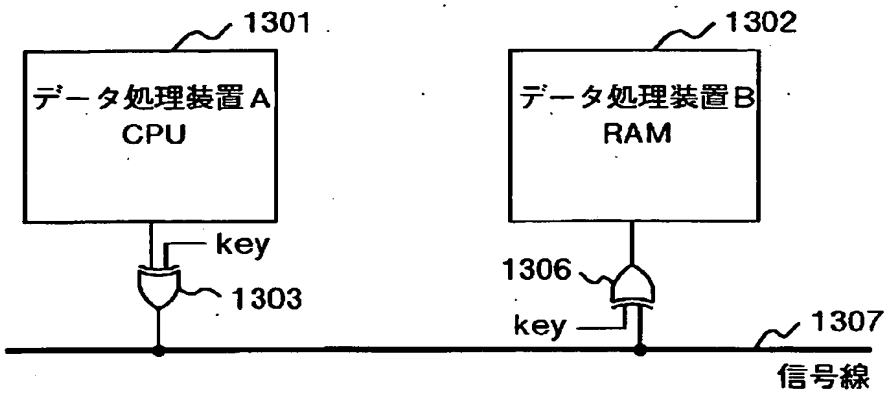
【図２６】

図　２６



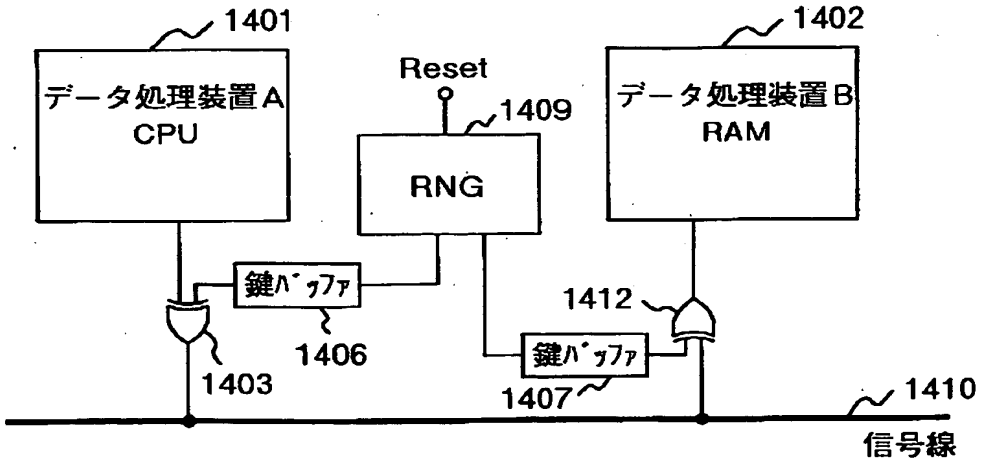
【図２７】

図　２７



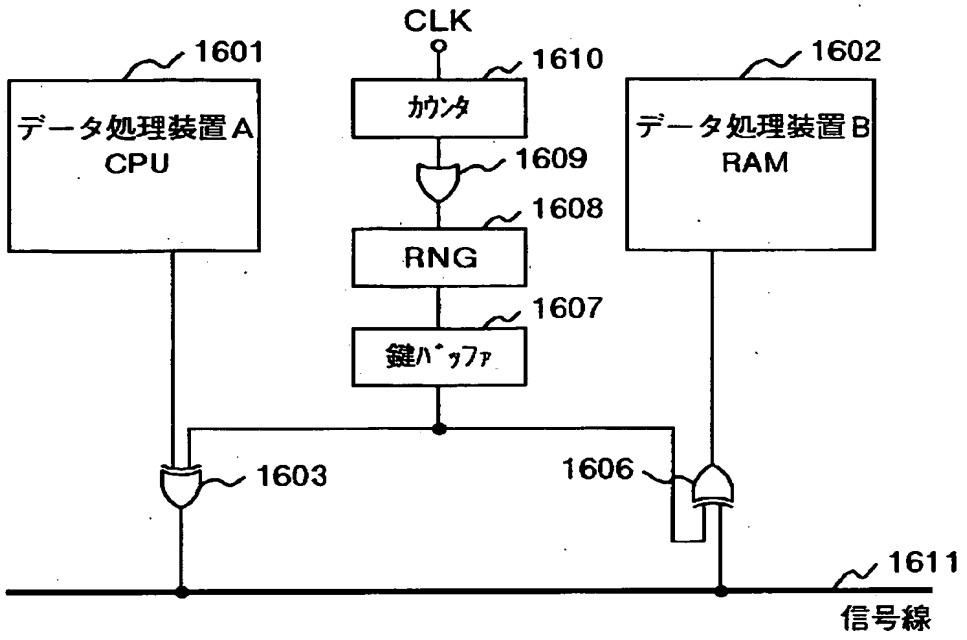
【図２８】

図　２８



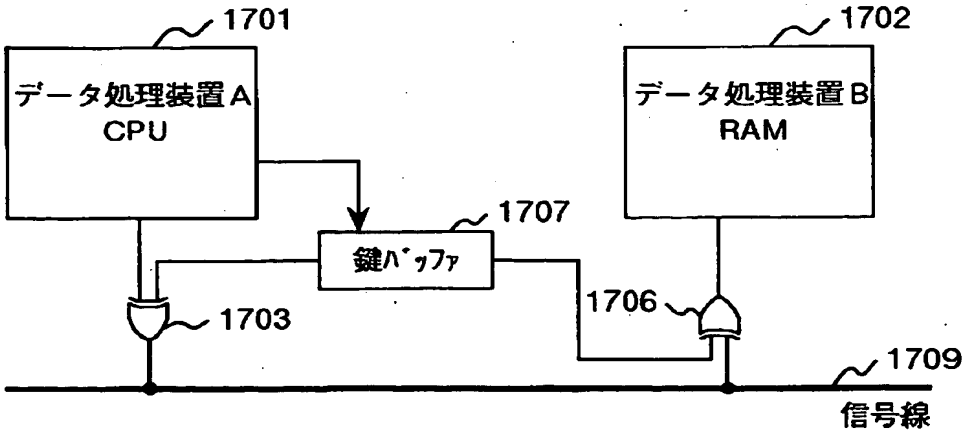
【図２９】

図　２９



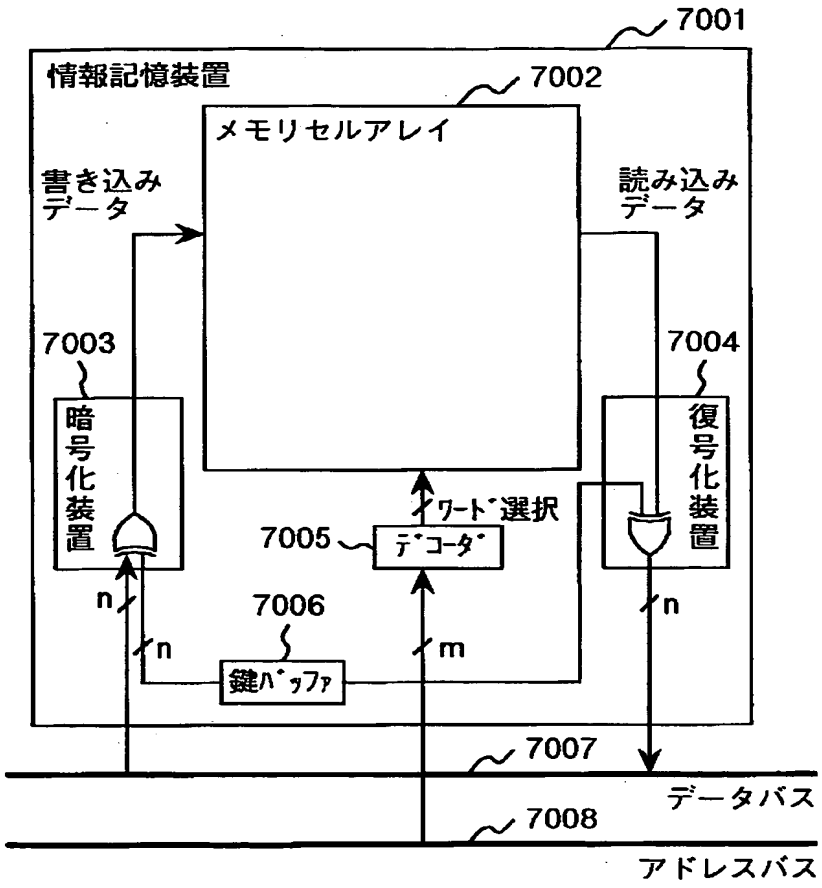
【図３０】

図　３０



【図３１】

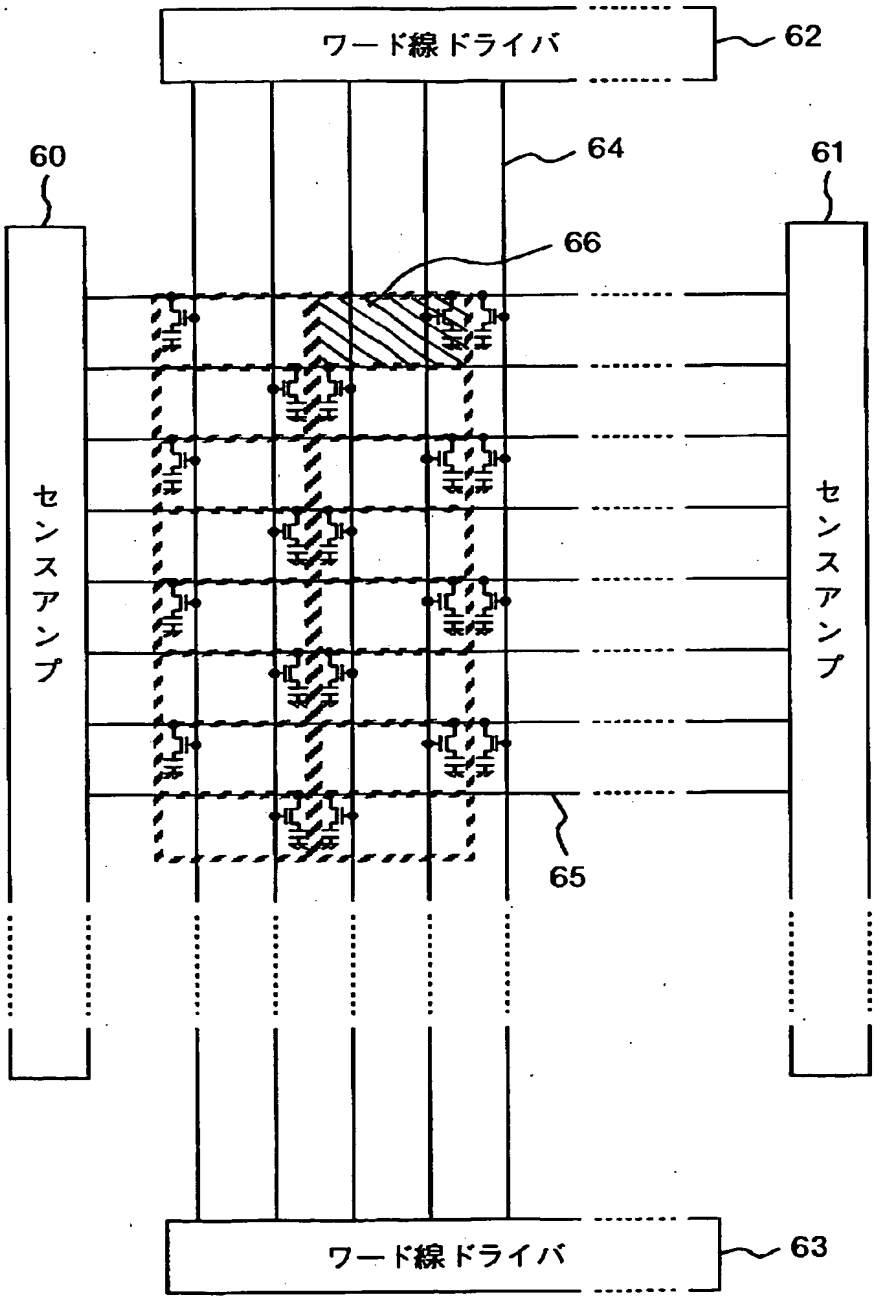
図　３１



出証特２０００－３０４５６５０

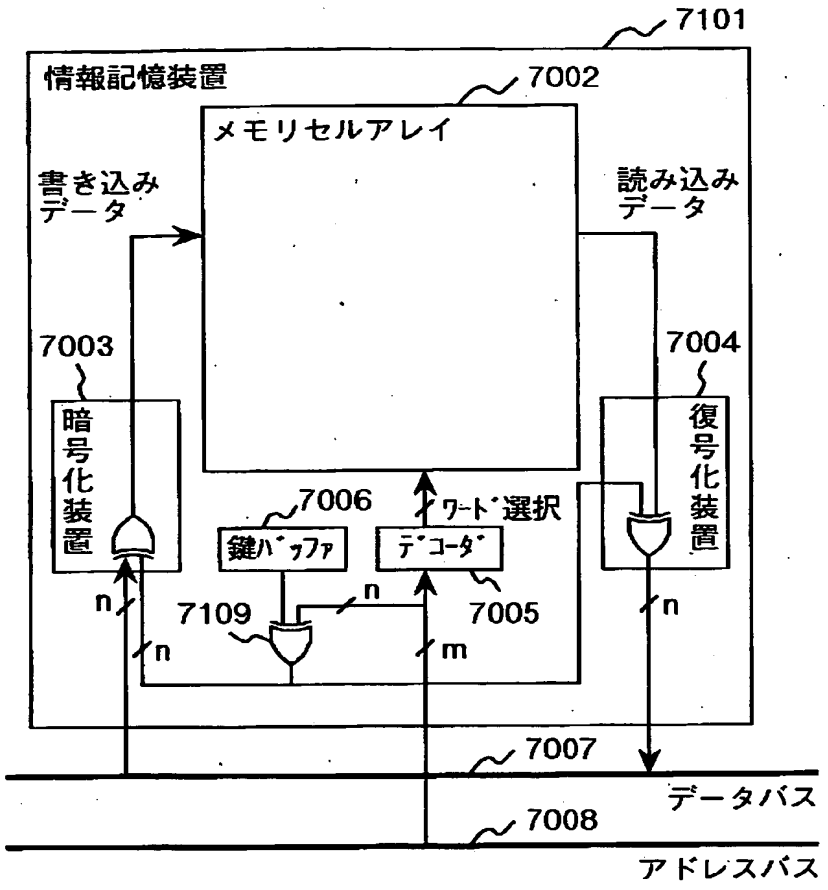
【図３２】

図　３２



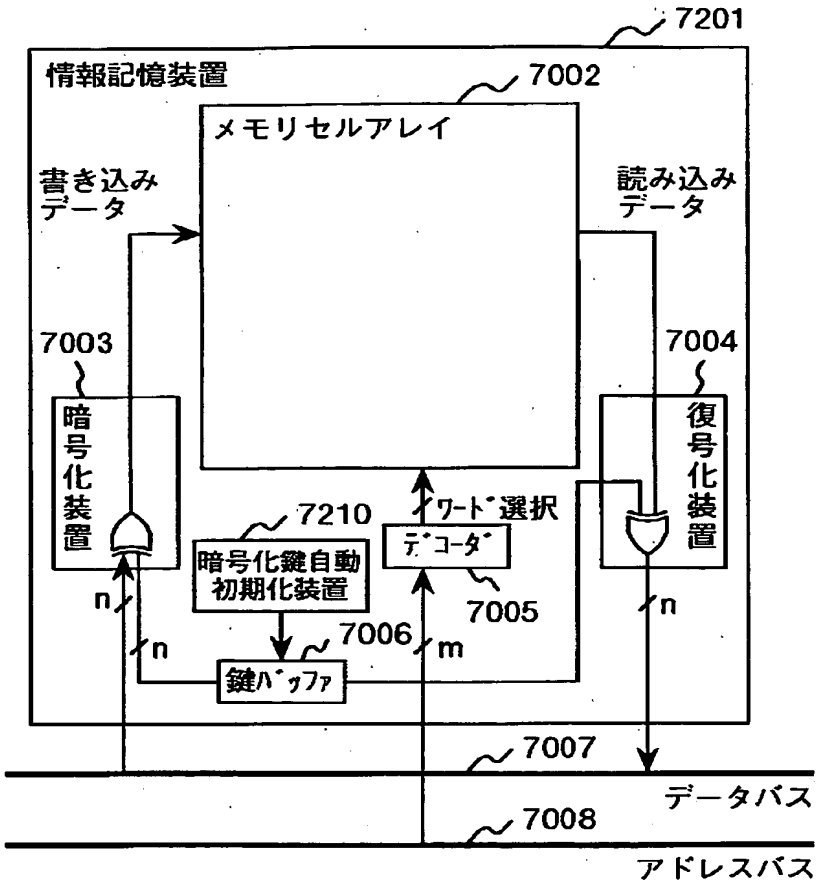
【図３３】

図　３３


7101
情報記憶装置
7002
メモリセルアレイ
書き込みデータ
読み込みデータ
7003
7004
暗号化装置
復号化装置
7006
鍵ﾊﾞｯﾌｧ
ﾜｰﾄﾞ選択
ﾃﾞｺｰﾀﾞ
7005
7109
n
m
7007
データバス
7008
アドレスバス

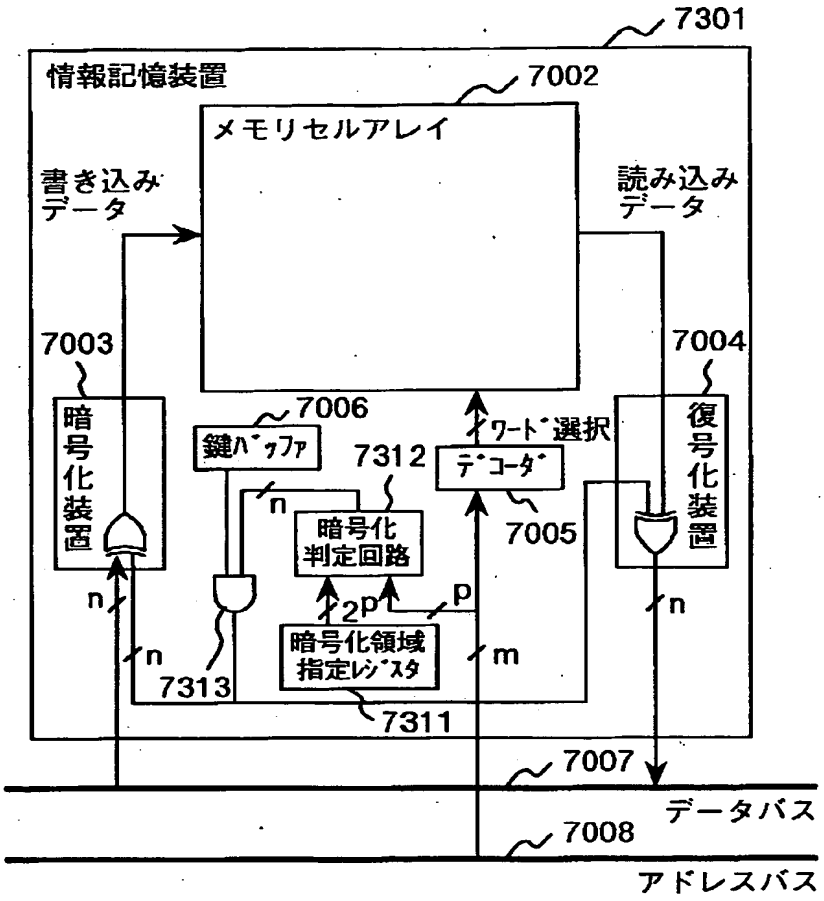
【図３４】

図　３４


7201
情報記憶装置
7002
メモリセルアレイ
書き込み
データ
読み込み
データ
7003
7004
暗号化装置
復号化装置
7210
暗号化鍵自動
初期化装置
ﾜｰﾄﾞ選択
ﾃﾞｺｰﾀﾞ
7005
n
n
7006
m
n
鍵ﾊﾞｯﾌｧ
7007
データバス
7008
アドレスバス

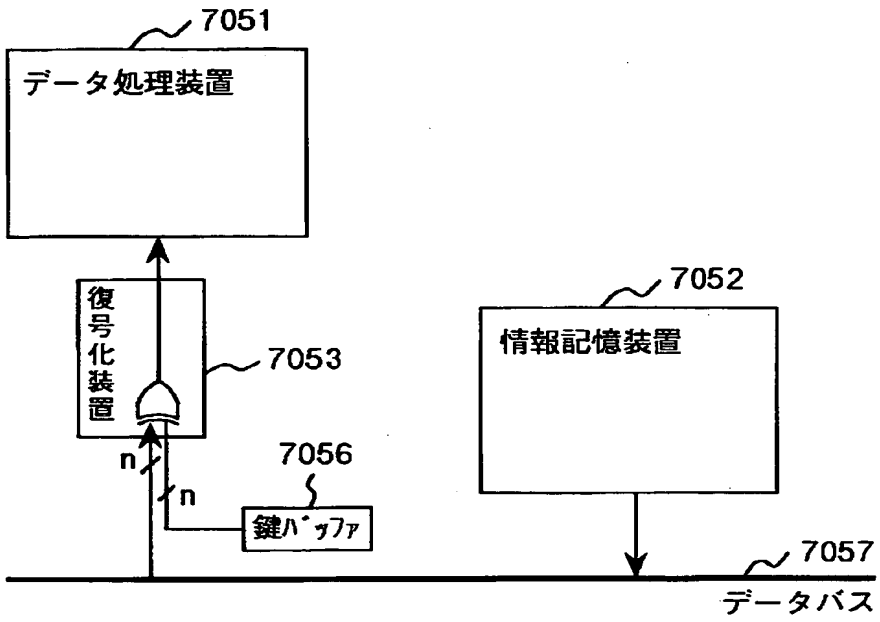
【図３５】

図　３５


7301
情報記憶装置
7002
メモリセルアレイ
書き込みデータ
読み込みデータ
7003
7004
暗号化装置
7006
鍵ﾊﾞｯﾌｧ
ﾜｰﾄﾞ選択
7312
ﾃﾞｺｰﾀﾞ
7005
復号化装置
暗号化判定回路
n
2p
p
暗号化領域指定ﾚｼﾞｽﾀ
m
7313
7311
7007
データバス
7008
アドレスバス

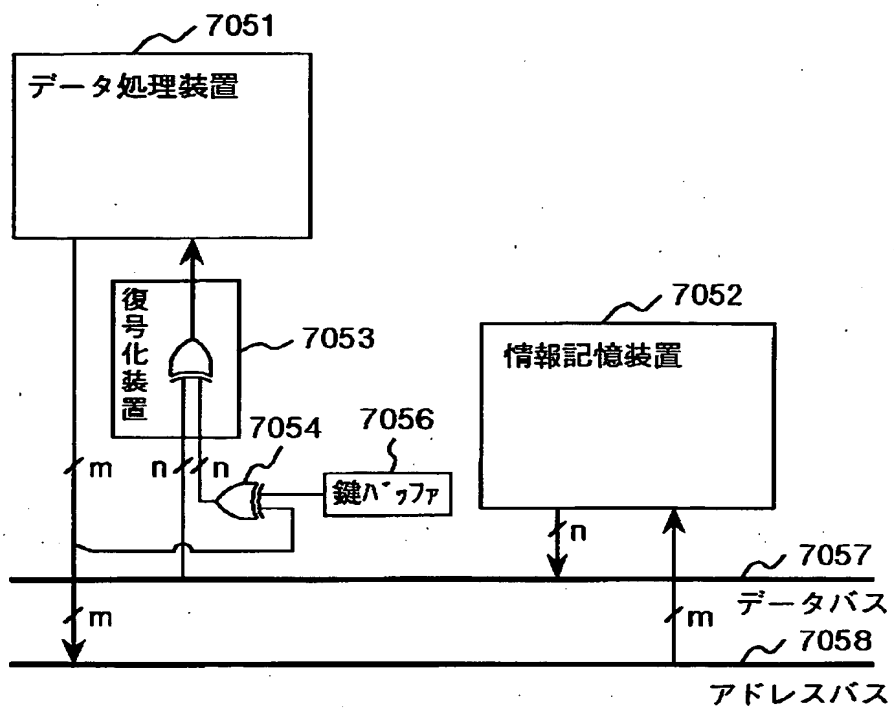
【図３６】

図　３６


7051
データ処理装置
復号化装置
7053
n
n
7056
鍵ﾊﾞｯﾌｧ
7052
情報記憶装置
7057
データバス

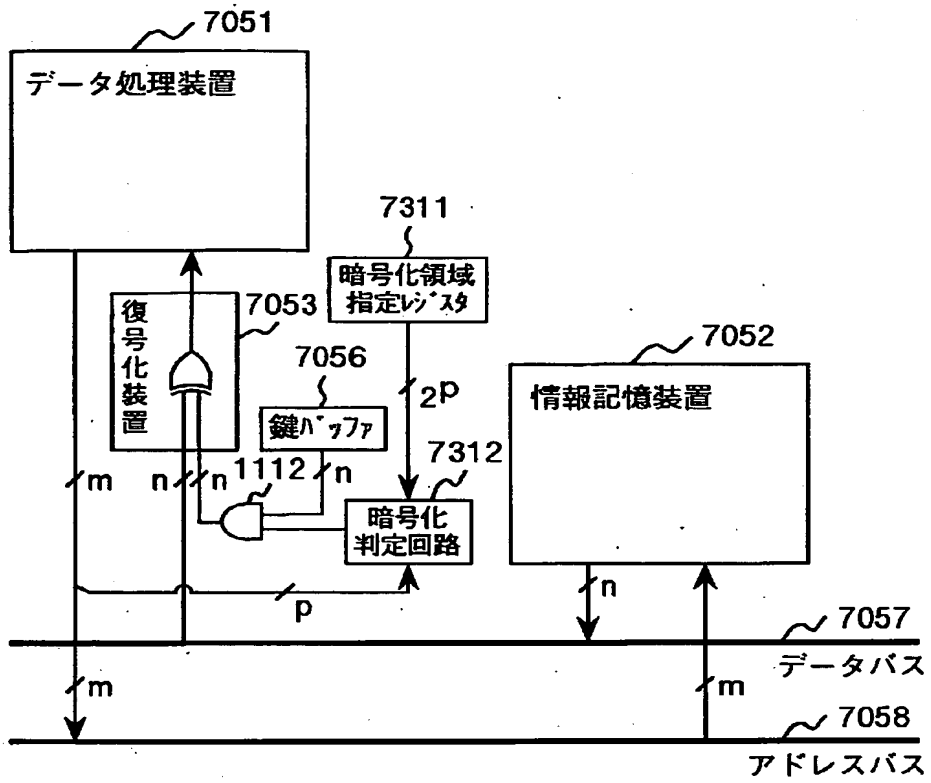
【図３７】

図　３７


7051
データ処理装置
復号化装置
7053
7052
情報記憶装置
7054
7056
m
n
n
鍵ﾊﾞｯﾌｧ
n
7057
データバス
m
m
7058
アドレスバス

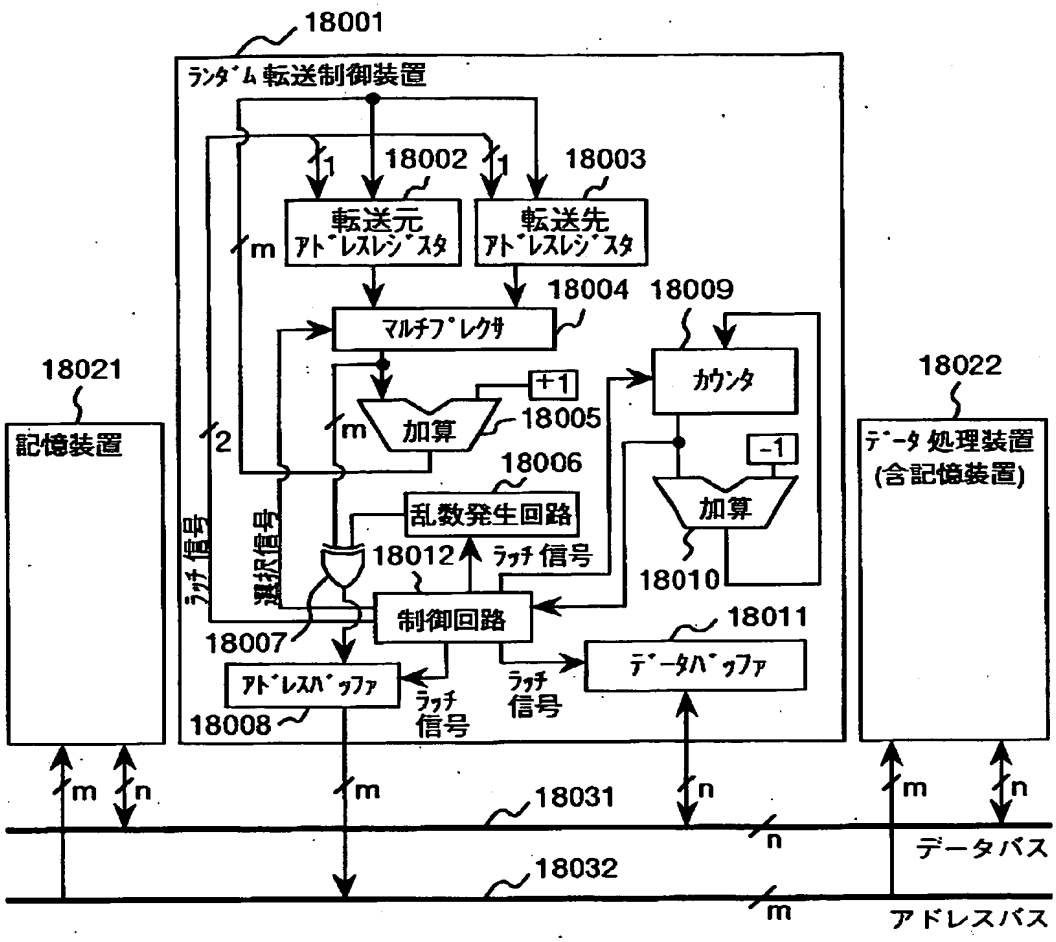
【図３８】

図　３８


7051
データ処理装置
7311
暗号化領域
指定ﾚｼﾞｽﾀ
復号化装置
7053
7056
鍵ﾊﾞｯﾌｧ
2p
7052
情報記憶装置
7312
m
n
n
1112
n
暗号化
判定回路
p
n
7057
データバス
m
m
7058
アドレスバス

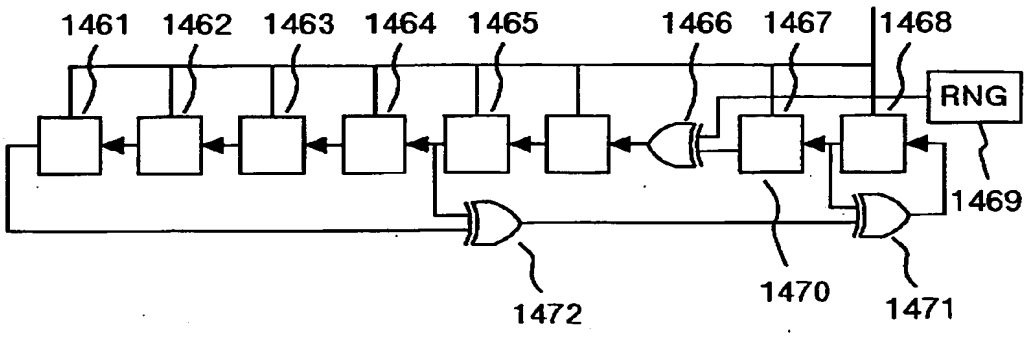
【図３９】

図　３９


18001
ﾗﾝﾀﾞﾑ転送制御装置
18002
18003
転送元
ｱﾄﾞﾚｽﾚｼﾞｽﾀ
転送先
ｱﾄﾞﾚｽﾚｼﾞｽﾀ
18004
18009
ﾏﾙﾁﾌﾟﾚｸｻ
ｶｳﾝﾀ
18021
記憶装置
18022
ﾃﾞｰﾀ処理装置
(含記憶装置)
+1
加算
18005
-1
加算
18006
乱数発生回路
ﾗｯﾁ信号
選択信号
18012
ﾗｯﾁ信号
18010
制御回路
18011
18007
ﾃﾞｰﾀﾊﾞｯﾌｧ
ｱﾄﾞﾚｽﾊﾞｯﾌｧ
ﾗｯﾁ
信号
ﾗｯﾁ
信号
18008
m
n
18031
データバス
18032
アドレスバス

【図４０】

図　４０


1461
1462
1463
1464
1465
1466
1467
1468
RNG
1469
1470
1471
1472

【書類名】要約書

【要約】

【課題】　本願発明は、高いセキュリティを持つ情報処理装置を提供せんとするものである。更には、本願発明は、高いセキュリティを持つカード部材、およびカード・システムを提供するものである。

【解決手段】　本願発明の形態は、情報処理装置と、当該第１の情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置よりの信号を伝達する前記信号線での電力の消費状態に対応して、この電力消費状態とは別の電力の消費が可能とされている情報処理装置である。本願発明の別な形態はあ、情報処理装置と、当該情報処理装置につながれた信号線とを少なくとも有し、前記情報処理装置と前記信号線との間において、前記情報処理装置よりの信号を暗号化が可能であり且つ前記信号線より暗号化されて転送される信号を復号化することが可能な情報処理装置である。更に、本願の別な形態は、情報処理装置と、情報記憶装置と、少なくとも前記情報処理装置につながれた信号線とを少なくとも有し、少なくとも前記情報記憶装置への情報の格納は当該格納すべき情報を暗号化してなされ、且つ前記情報記憶装置に格納された情報の復号化が可能な情報処理装置である。

【選択図】図５

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

出　願　人　履　歴　情　報

識別番号　　〔０００２３３１６９〕

１．変更年月日　　１９９８年　４月　３日
［変更理由］　名称変更
住　所　東京都小平市上水本町５丁目２２番１号
氏　名　株式会社日立超エル・エス・アイ・システムズ